目　录

第一章 系统概述 1
1.1 系统简介 1
1.2 系统结构和组成 3
1.3 运行环境 4
1.4 主要功能 4
1.5 可管理服务器类型 6

第二章 快速入门 7
2.1 快速安装、配置和运行 7
2.1.1 安装前的准备工作 7
2.1.2 首次安装和配置 7
2.1.3 首次运行 8
2.2 基本操作 9
2.2.1 登录 9
2.2.2 搜索服务器 9
2.2.3 添加服务器 10
2.2.4 监视和控制服务器 12
2.2.5 查看服务器事件 13
2.2.6 接收服务器告警 13

第三章 规划和部署 15
3.1 单服务器管理 15
3.2 Intranet 内多服务器集中管理 16
3.3 跨 Internet 的多服务器集中管理 17

第四章 安装与卸载 19
4.1 安装管理中心 19

4.2 安装管理代理 20
4.2.1 安装 Window 下的管理代理 20
4.2.2 安装 Linux 下的管理代理 21
4.3 安装远程控制工具 22
4.4 卸载管理中心 23
4.5 卸载管理代理 23
4.5.1 卸载 Window 下的管理代理 23
4.5.2 卸载 Linux 下的管理代理 23
4.6 卸载远程控制工具 23

第五章 配置 24
5.1 基本概念 24
5.2 服务器管理代理配置 25
5.2.1 Window 下的配置 25
5.2.2 Linux 下的配置 29
5.3 管理中心配置 32
5.3.1 基本配置 32
5.3.2 高级配置 35
5.4 管理员浏览器的配置 38
5.5 BMC 配置 38
5.5.1 BMC 出厂设置 38
5.5.2 设置 BMC 40

第六章 功能概述 41
6.1 主界面 41
6.2 基本功能 42
6.2.1 服务器管理 42
6.2.2 服务器监视和控制 42
6.2.3 服务器事件管理 43
6.2.4 服务器带外管理 44

6.2.5 服务器远程控制 45

第七章 服务器组织管理 46
7.1 功能简介 46
7.2 界面概述 46
7.3 基本操作 47
7.4 服务器搜索 47
7.5 服务器信息管理 49
7.6 服务器组管理 51
7.7 历史信息存储 52
7.7.1 基本操作 52
7.7.2 分析历史信息 53

第八章 服务器监控管理 54
8.1 功能简介 54
8.2 界面概述 54
8.3 基本信息 55
8.4 服务器监视 56
8.4.1 性能信息 56
8.4.2 资产信息 58
8.4.3 硬件健康信息 61
8.5 服务器控制 62
8.5.1 阈值设置 62
8.5.2 服务器控制 63
8.6 事件管理 64
8.7 告警策略配置 65

第九章 服务器事件管理 66
9.1 功能简介 66
9.2 界面概述 66

9.3 基本操作 67
9.4 事件过滤 69
9.5 事件确认 70
9.6 事件导出 70
9.7 事件告警 70
9.7.1 浏览器页面告警 71

第十章 日志管理 72
10.1 功能简介 72
10.2 界面概述 72
10.3 基本操作 73
10.4 日志过滤 73

第十一章 用户管理 75
11.1 功能简介 75
11.2 界面概述 76
11.3 基本操作 76
11.4 用户权限分配 78
11.5 权限控制 80

第十二章 告警策略配置 81
12.1 功能简介 81
12.2 界面概述 81
12.3 发送短信警报 83
12.4 电子邮件警报 83
12.5 发送 SNMP Trap 警报 85

第十三 系统配置管理 86
13.1 功能简介 86
13.2 界面概述 86

13.3 日志保存策略配置 88
13.4 事件记录保存策略配置 88
13.5 系统缺省每页显示的记录数 88
13.6 系统邮箱参数配置 88
13.7 GSM Modem 参数配置 89
13.8 系统密码策略 90
13.9 监控刷新频率配置 90

第十四章 通讯录 91
14.1 功能简介 91
14.2 界面概述 91
14.3 基本操作 92

第十五章 服务器远程控制工具 93
15.1 功能简介 93
15.2 界面概述 93
15.3 IDE 重定向 95
15.3.1 生成 IDE 重定向证书 95
15.3.2 设置服务器 BIOS 97
15.3.3 IDE 重定向 97
15.4 串口重定向 98
15.4.1 设置服务器 BIOS 98
15.4.2 配置 BMC 芯片 99
15.4.3 SOL 100

第十六章 BMC 配置 101
16.1 Get 命令说明 103
16.1.1 获取当前网络配置 103
16.1.2 获取当前 SOL 配置 104
16.2 Set 命令说明 104

16.2.1 配置网络 104
16.2.2 设置 BMC 管理密码 105
16.2.3 配置 SOL 106
16.3 帮助命令说明 106
16.3.1 Help 命令 106
16.3.2 内部命令的帮助 107

第十七章 常见问题解答（FAQ） 108
17.1 安装与卸载 108
17.2 运行与配置 108
17.3 服务器搜索 108
17.4 服务器监控 109
17.5 事件与告警 110
17.6 用户与权限 111
17.7 系统配置 111
17.8 和浏览器相关的问题 111
17.9 服务器远程控制 112

附录 A 术语 113

第一章 系统概述

1.1 系统简介

联想万全慧眼III专业版（Lenovo SureEyes III）作为联想万全慧眼服务器系统监控软件的第三代产品，是面向企业用户，提供企业网范围内的多台联想服务器集中远程监控管理的解决方案。

联想万全慧眼系统III专业版（以下简称SureEyes3）采用了全新的软硬件架构，是符合目前服务器监控管理的业界标准——智能平台管理接口（IPMI）规范v2.0的服务器监控管理软硬件解决方案。

SureEyes3用于管理本地和远程的联想万全服务器，可实现服务器故障报警、系统资源管理以及系统性能监控等多种功能。SureEyes3采用业界领先的B/S架构，由万全慧眼管理中心（SureEyes Manager）和管理代理（SureEyes Agent）两部分组成。安装了万全慧眼管理中心后，管理员就可以通过浏览器登录到管理中心对局域网中和可达的广域网中所有安装有万全慧眼管理代理的联想万全服务器进行远程监控，轻松掌握各服务器的健康状况信息。当系统出现故障时，可自动实现远程和本地报警，并将警告事件记录到系统中。用户可检索并分析系统中存储的事件信息，及时发现并排除系统可能出现的故障，保证联想万全服务器长期稳定、可靠地运行。

此外，对于具备BMC芯片的服务器，用户还可以通过远程控制工具（SureEyes Remote Control Utility）将本地IDE设备虚拟成远程服务器的IDE设备，并通过IPMIv2.0定义的SOL（Serial over LAN，基于网络的串口重定向）功能远程接管服务器的开机过程。

BMC（Baseboard Management Controller主板管理控制器）是内置在部分万全服务器主板上的一颗管理芯片。有了这颗BMC芯片，无论服务器操作系统状态如何，无论服务器是开机还是关机，只要电源供电，就可以通过系统网络直接和被管服务器的BMC交互，获取服务器硬件健康信息和事件，并且可以对服务器进行关机、开机和重启、点亮ID灯、前面板锁定等操作，为及时定位和排除故障提供了有力的帮助。这样管理软件做到和操作系统无关，实现了目前业界最先进的带外管理（Out-Of-Band Management）。而在传统方式下，实现带外管理需要用户在服务器上配置昂贵的专用设备。

万全慧眼对管理员的技术水平要求不高，并且大大减轻了管理人员的劳动负担，可显著提高服务器的可管理性，缩短服务器的非正常停机时间，从而有效降低服务器的总体拥有成本（TCO）。

SureEyes3 的全新特性包括：

全新的软硬件解决方案

- 对于主板集成了BMC（Baseboard Management Controller）芯片的服务器，全面支持其基于系统网络的带外管理，无需外插管理卡，为用户提供便利的服务器管理方案。
- 管理软件采用全新的架构、全新的界面设计，为用户提供更人性化、更易用、更安全的大规模服务器集中管理。

强大的管理功能

- 强大的带外管理功能：对于具有BMC芯片的服务器，无论其OS状态如何（正常、宕机、非主流操作系统），无论服务器是开机还是关机，只要电源供电，就可以通过网络直接和被管服务器的BMC交互，获取服务器硬件健康信息和事件，并且可以对服务器进行关机、开机和重启、点亮 ID 灯、前面板锁定。
- 独立的管理代理可以支持对带 BMC 和不带 BMC 的服务器的资产配置、资源使用、性能信息、进程信息等的远程管理，并且可以对关键部件设置阈值进行报警。
- 多种用户可选的告警方式：短信、邮件、颜色变化、SNMP Trap。
- SOL（Serial Over LAN，基于网络的串口重定向）：对于具有 BMC 芯片的服务器，可以做到 POST 过程重定向、BIOS 远端设置、远程登录到 DOS。
- IDER（IDE Redirection）：对于具有 BMC 芯片的服务器，可以将控制台的光驱、软驱重定向到被管服务器端。同时，借助SOL功能，进行远程BIOS、驱动升级、启动到 DOS 进行诊断等功能。
- 可以记录进程等历史信息；在服务器宕机后，可以用于分析宕机原因。
- 完备的历史信息和事件的导出功能，可导出为文本文件或 Excel 格式文件。
- 通过一个管理中心，用户最多可以同时管理 128 台服务器。

完备的安全机制

- 使用用户认证授权机制确保只有合法用户访问本系统。
- 系统管理员可以根据需要增加管理用户，赋予不同的用户级别和管理权限，

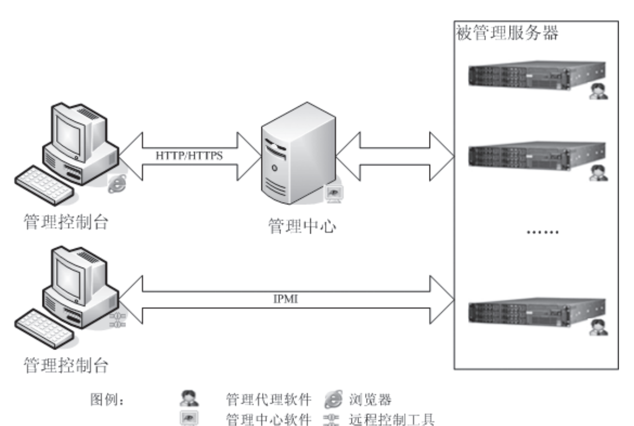
增加系统管理的安全性。
- 用户的操作有系统日志做详细记录。
- 管理中心和服务器之间采用安全的私有通信协议,避免系统遭到针对SNMP的攻击。
- 用户可以使用 https 方式从浏览器访问管理中心，确保通信安全。
- 前面板接管：可以对前面板进行锁定，防止用户误操作。
- 对于服务器插拔 USB 盘、热插拔硬盘等重要操作，系统会产生告警事件。

全新的易用性设计
- 全新界面设计，设计更加人性化，使用更方便。
- 零客户端安装,基于网络浏览器的用户访问界面,用户可以从网络可达的任何地方登录和管理服务器。
- 基本硬件监控和带外管理采用主板集成BMC,不需额外安装管理卡和连线。

1.2 系统结构和组成

SureEyes3 软件包括以下几个部分：
- 管理中心软件
- 管理代理软件
- 客户端浏览器（由用户自行提供）
- 服务器远程控制工具软件

下图展示了 SureEyes3 的的管理模式。



管理代理安装在被管的服务器上，通过操作系统和主板集成的BMC控制器对被管理服务器的各项物理指标进行数据采集、发送到网络中指定的管理中心，并执行来自管理中心的控制指令；管理中心通过对来自管理代理的信息进行处理和分析，为管理者提供一个全面的系统监控解决方案。

此外，管理员可以通过Internet浏览器登录管理中心对服务器进行管理，也可以通过使用远程控制工具实现对被管理服务器的简单远程接管。

1.3 运行环境

本软件各个部分的运行环境说明如下：

SureEyes3管理中心软件	可以运行在台式机或者服务器上。支持的操作系统包括：Windows 2000 Server / Advanced Server SP4，Windows XP Professional，Windows 2003 Server Standard/ Enterprise Edition SP1
服务器管理代理软件	运行在被管理的联想万全服务器上，支持的操作系统包括：Windows 2000 Server/ Advanced Server SP4，Windows 2003 Server Standard/ Enterprise Edition SP1（32bit/64bit），Linux RedHat 9.0，Linux RedHat Enterprise Linux AS3.0, Linux RedHat Enterprise Linux AS4.0（32bit/64bit）
客户端浏览器	Windows操作系统或者Linux操作系统， IE6以上或者Firefox1.5以上
服务器远程控制工具	运行在Windows 2000以上的操作系统的台式机或者服务器之上

1.4 主要功能

1. 服务器组织管理

在SureEyes3中服务器是通过管理视图被组织起来的。管理视图结构以列表的形式显示出当前可以被控制监视的所有联想服务器。管理视图结构不仅提供直观的服务器运行状况概览，而且能够使得管理员方便地针对某台具体的服务器进行细致的监视和控制。服务器管理为管理员提供三项主要的功能：服务器维护、管理视图维护和服务器搜索。

2. 服务器监控管理

管理员可以监视服务器的多种信息，包括：服务器基本信息、资产信息、性能

信息、健康信息。管理员还可以设定服务器阈置，并远程控制服务器，包括：远程开关机和重启、点亮 / 熄灭服务器的 ID 灯和前面板软件锁定 / 解锁。

此外，对于监视的服务器，用户可以选择是否进行信息存储，以保存服务器进程运行状态的历史记录，并可以导出存储的数据。

3. 服务器事件管理

SureEyes3记录并保存了服务器产生的各种事件信息，为用户提供丰富的事件管理功能。

事件信息可以通过以下两种方式进行采集获得：

- 如果被管服务器在开机的状态下，并且运行了管理代理，则管理中心会接收来自管理代理发送的事件。
- 如果被管服务器在关机的状态下，但电源未关闭，并且保持有网络连接，则管理中心会定时主动轮询服务器，从而获得事件。

管理员可以对所有存储的事件信息进行浏览、查询、导出等操作。

管理员还可以对事件设置告警策略，指明在何种情况下生成一条告警，并采取何种方式通知管理人员。告警的方式有短信通知、Email 通知、SNMP Trap 通知、浏览器界面通知。

- 短信：通过放置在管理中心上的短信硬件模块（选件）发送短信息；
- 电子邮件：通过管理中心可以连接的 SMTP 服务器发送电子邮件；
- SNMP Trap：向指定的 IP 地址列表发送 SNMP Trap 形式的告警；
- 浏览器界面通知：浏览器界面定时刷新获得当前事件所表示的服务器运行状态；

4. 系统管理

系统管理包括日志管理、用户权限管理、系统配置。

日志信息主要是管理员对服务器的控制操作信息，开机关机信息，管理员登录系统的记录信息等。

用户权限管理负责系统的用户管理和权限认证，合理向用户分配所需的操作权限，保证各用户能并且只能执行授权的操作。

系统配置提供对系统的各种运行参数的配置功能，包括：日志保存存储策略、事件记录保存策略、系统缺省每页显示的记录数、系统邮箱参数配置、GSM Modem 配置、系统密码策略、监控刷新频率配置。

5. 服务器远程控制工具

服务器远程控制工具的功能包括IDER（IDE设备重定向）和SOL（基于网络的串口重定向）。

IDE设备重定向主要是将远程控制工具所在的主机的IDE设备通过网络重定向至服务器，使没有软驱或光驱的服务器可以从该主机的软驱或光驱引导系统。

串口重定向主要是将服务器的串口信息通过网络重定向至远程控制工具所在的主机，使用户可以远程操作服务器，包括查看服务器的POST过程、进行BIOS设置以及接管DOS系统操作。

通过服务器远程控制工具，可以方便管理员进行服务器故障远程在线诊断。

该工具仅对于具有BMC芯片的服务器有效。

1.5 可管理服务器类型

SureEyes3可以管理包括联想万全服务器、非联想服务器、PC在内的大量主机设备。如果用户使用的万全服务器具有BMC芯片，那么还可以进行带外管理、SOL和IDER。

第二章 快速入门

2.1 快速安装、配置和运行

2.1.1 安装前的准备工作

在使用万全慧眼对服务器进行管理之前，建议用户对管理的模式进行规划。规划的时候首先需要了解当前或者即将部署的服务器所处的网络拓扑结构，然后需要规划管理中心部署的位置和方式。典型的，用户需要在一台专门的服务器或者 PC 上部署管理中心。具体的规划和部署方法参见 3 *规划和部署*。

在第一次安装 SureEyes3 之前，首先服务器需要安装好操作系统，接着如果用户希望启用带外管理功能，还需要对服务器的 BMC 管理芯片进行初始化配置。主要就是配置带外管理帐户，以及带外管理的 IP 地址、子网掩码和网关。具体的配置方法参见 5.5BMC 配置。

注意：进行带外管理之前，必须确认服务器具有 BMC 芯片。

2.1.2 首次安装和配置

2.1.2.1 安装管理中心

首先，用户需要在一台安装 Windows 操作系统的机器（服务器或者 PC 机）上安装管理中心。安装之前请确认该机器具有至少512M内存和1G以上磁盘空间。插入 Sureeyes3 光盘，安装程序自动运行，选择“安装管理中心”，或者运行位于安装光盘manager目录下的管理中心安装程序SureEyes3-Manager-xxxxxx.exe，全部选择默认选项。安装完毕，弹出管理中心配置窗口，采用默认配置，按下确认按钮。最后用户从 Windows 托盘区中通过管理中心托盘程序启动管理中心。

详细的安装过程参见 4.1 *安装管理中心*。

安装完成后，用户需要确认防火墙正确配置，允许管理中心作为例外的程序运行，或者使用特定的网络服务端口。具体配置方法参见 5.3.1.4 *管理中心防火墙配置*。

2.1.2.2 安装管理代理

接着，用户依次在需要管理的服务器上安装管理代理。插入 Sureeyes3 光盘，安装程序自动运行，选择“安装管理代理”；或者运行位于安装光盘的agent目录下的管理代理安装程序。根据服务器操作系统的不同，windows 下是 SureEyes3-Agent-xxxxxx.exe，Redhat Linux 下是 sureeyesagentd-3-2.4.X.X.i386.rpm（2.4 内核）或者 sureeyesagentd-3-2.6.X.X.i386.rpm（2.6 内核）。

如果服务器运行Windows操作系统，运行代理安装程序，全部选择默认选项。安装完毕，弹出管理代理配置窗口，修改“事件发送目标地址”为管理中心所在的IP地址，目标端口不变。确认后，在询问是否启动代理的对话框中选择是，即可启动管理代理。

如果服务器运行 Linux 操作系统，使用 rpm 命令运行代理安装程序：

rpm -ivh sureeyesagentd-3-2.4-XX.i386.rpm（用于内核版本为2.4的Linux）

或者

rpm -ivh sureeyesagentd-3-2.6-XX.i386.rpm（用于内核版本为2.6的Linux）

安装完毕，使用

service sureeyesagentd set

命令进入代理配置程序。输入数字 4，设置管理中心的 IP 地址，端口号不变。然后输入数字 99，保存退出，系统询问是否重启管理代理，选择“是”。

安装完成后，用户需要确认防火墙正确配置，允许管理代理作为例外的程序运行，或者使用特定的网络服务端口。分别参见5.2.1.5*Windows 下的管理代理防火墙配置*和 5.2.2.4*Linux 下的管理代理防火墙配置*。

详细的安装过程参见 4.2 *安装管理代理*，配置方法参见 5.2 *配置管理代理*。

2.1.3 首次运行

快速安装完毕，用户可以从任何一台能够联网到管理中心的机器访问管理中心。用户打开使用的机器的浏览器（要求至少是IE6或者FireFox1.5以上），在URL地址栏输入

http://<管理中心 IP>:8898

即可进入管理中心的登录页面。

用户输入帐号admin，口令admin123即可成功登录，进入管理中心的主界面。

此后，用户可以根据 2.2 *基本操作*的说明进行首次使用。

2.2 基本操作

2.2.1 登录

如前所述，安装完管理中心并启动完毕后，默认情况下，用户可以通过在浏览器中输入 URL 地址：http://< 管理中心 IP>:8898 打开登录页面。



默认地，用户输入帐号 admin，口令 admin123，登录 SureEyes3 管理中心。

用户第一次登录后，建议立即修改admin帐号的口令，在页面下方的状态栏点击当前用户帐号可以修改口令。默认地，口令不能与帐号名称重复，必须含有字母和数字，长度大于 6 位。

2.2.2 搜索服务器

在第一次使用 SureEyes3 的时候，用户首先要搜索和添加待管理的服务器。

在搜索之前，请确认待管理的服务器都已经插上电源，并且都安装并运行了管

理代理。如果用户修改了代理的默认端口和通信密钥，则需要事先在管理中心做相应的修改。具体的配置方法参见 5.3.1.3 *配置管理中心参数*。

用户点击服务器管理视图中的“服务器搜索”链接，可以进入服务器搜索功能界面。

您的位置：服务器管理--搜索服务器--新近发现的服务器列表

新搜索

最近一次搜索没有发现任何新的服务器或新发现服务器已被加入管理列表。如需要，请发起新搜索。

新发现服务器列表

名称	带内管理IP	带外管理IP	发现时间	明细	添加到服务器列表

可更新服务器列表

名称	带内管理IP	带外管理IP	对应服务器明细	明细	更新到服务器列表	删除
lenovo-zmo6jq0f	172.100.1.25				更新	×
testserver1	172.100.1.26				更新	×

根据发现的服务器是否已经存在于被管理服务器中，服务器搜索功能界面分为新发现服务器和可更新服务器两个列表，可针对这两个不同列表中的服务器进行不同的操作。对新发现服务器列表中的服务器，可以选择将服务器增加到被管理服务器列表中；对可更新服务器列表，则可以选择将本次搜索时得到的结果更新到被管理服务器中对应的服务器上，也可以选择删除此条可更新服务器记录忽略此次的搜索结果。

点击“新搜索”按钮，可以发起一次新的搜索任务。通过填写开始和结束的IP地址，可以对指定的网段进行一次搜索。如果只填写开始或结束 IP 地址，则被认为是搜索填写的单个 IP 地址。一次搜索的地址范围不能超过 256 个有效 IP 地址。

用户可以通过从可供选择的历史搜索范围中选择前几次的搜索范围，可供选择的历史搜索范围中保存了最近 10 次搜索任务的地址范围记录。

提示：对于同一个管理中心，在同一时间只能有一个用户进行搜索操作，其他用户必须等待当前的搜索结束后才能开始新的搜索。在等待的时候，搜索页面显示一个搜索进度条，功能被阻止使用。

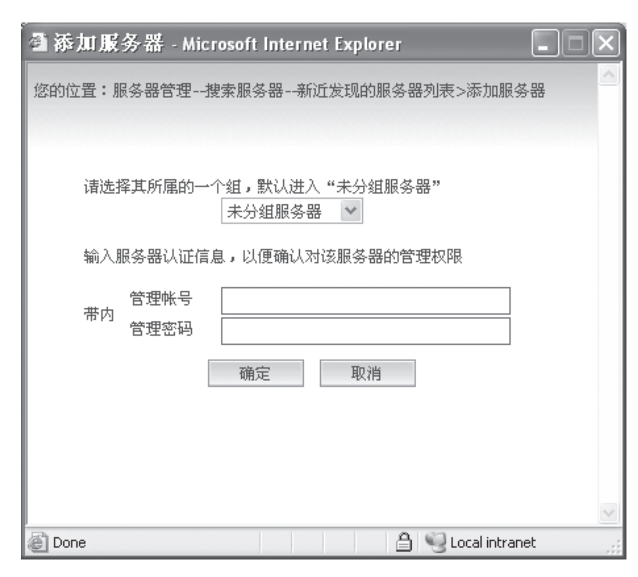
搜索服务器操作的详细说明参见 7.4 *服务器搜索*。

2.2.3 添加服务器

当服务器搜索结束后，如果发现了新的服务器，即会在新发现服务器列表中显

示出新的服务器，此时便可以添加服务器到管理列表中去了。

点击该服务器的添加链接即会弹出添加服务器对话框。



添加服务器时，需要选择将服务器添加到的服务器组（缺省为未分组服务器组）。同时必须填写对该服务器进行管理的带内管理帐号/密码和带外管理密码，以便将服务器添加到被管服务器中后可以正常管理服务器。默认地，被管理服务器的带内管理帐号是 sureeyes，密码是 sureeyes999；带外管理密码是 lenovo。



提示：带内管理帐号是指运行在被管理服务器上的管理代理设定的帐号；带外管理密码是指被管理服务器 BMC 的管理密码。

提示：被管理服务器的带内管理帐号口令可以通过管理代理的配置程序进行修改。请分别参见 5.2.1.4*Windows 下管理代理的认证参数配置*和 5.2.2.1*Linux 下管理代理的认证参数配置*。被管理服务器的带外管理密码需要使用 16*BMC 配置工具*进行修改。

添加服务器的详细说明参见 7.4 *服务器搜索*。

2.2.4 监视和控制服务器

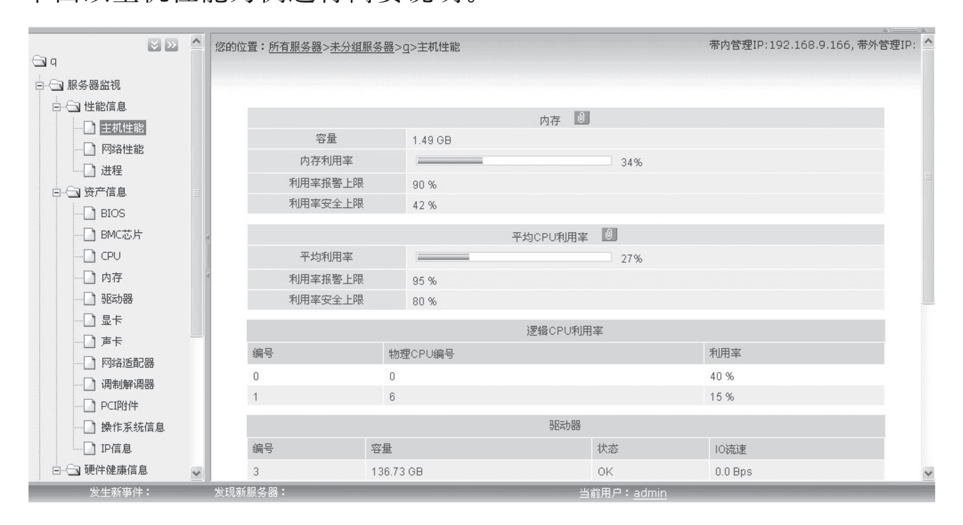
服务器添加完毕，就可以对它进行监控了。

在服务器管理界面选择一台服务器，点击其服务器名称上的链接，即可进入服务器监视界面。

进入服务器监视界面后，首先显示的是服务器的基本信息页面。用户可根据不同的需要点击功能节点区中不同的监视项目查看不同的服务器信息。

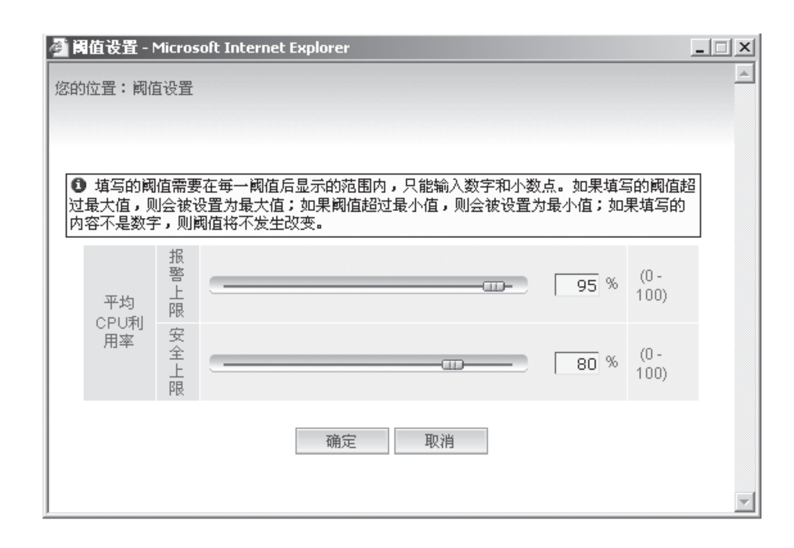
用户可以对服务器进行各种控制，设置各类阈值。

下面以主机性能为例进行简要说明。



服务器主机性能监视界面中显示了内存、CPU、磁盘的各类性能指标。

在“平均CPU利用率”后显示有图标 ，说明此监视项目可以设置阈值。点击图标 将弹出阈值设置窗口。



通过拖动滑动杆或直接输入阈值数值进行阈值设置，当设置完成后点击“确定”按钮最终确认设置，即可完成对该服务器的阈值设置。

2.2.5 查看服务器事件

用户在管理服务器的过程中，随时可以查看服务器发生的事件。如果被管理服务器发生了事件，将会在状态区的发生新事件栏出现一个闪动的图标，提示用户有新事件发生。用户点击该图标，可以进入事件管理，查看最新发生的事件。

用户可以查看事件的详情，可以点击服务器名称的链接，查看该服务器的事件信息。

对于查看过的事件，用户可以加以确认。

2.2.6 接收服务器告警

SureEyes3为服务器管理员提供了丰富的报警功能。在使用这些功能之前需要事先进行配置。

首先，在以管理员（例如admin）的身份登录管理中心后，通过左侧的导航树进入系统配置页面。在系统配置页面用户可以配置系统邮箱参数和GSM Modem参数。具体配置说明参见13 *系统配置*。用户可以通过测试按钮确认是否配置成功。配置完毕，用户就可以使用邮件告警和短信告警功能了。

接下来，用户需要设置告警策略。管理员用户通过左侧导航树节点进入告警策略配置页面。在该页面，用户可以配置多种告警方式的告警策略。具体配置说明参见 12 *告警策略配置*。

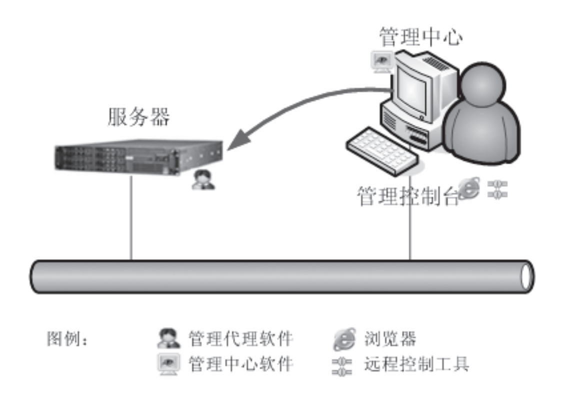
告警策略设置完毕，用户就可以通过不同的方式收到符合预定条件的告警事件了。

第三章 规划和部署

SureEyes3是一款集中服务器管理软件，既能够用于管理单台服务器，也能够用于管理网络中多台服务器（建议不超过128台服务器）。在您安装和使用SureEyes3之前需要根据您的具体情况进行规划和部署。以下针对几种典型的场景下的规划和部署进行说明。

3.1 单服务器管理

SureEyes3用于管理单台服务器是最简单的情况。



该场景下，管理控制台通过网络或者直连线与被管理服务器连接。

提示：管理控制台是指管理员远程管理服务器的位置。通常，用户在管理控制台通过Internet浏览器登录到管理中心，进行服务器管理。用户也可以在管理控制台使用远程控制工具对服务器进行管理。

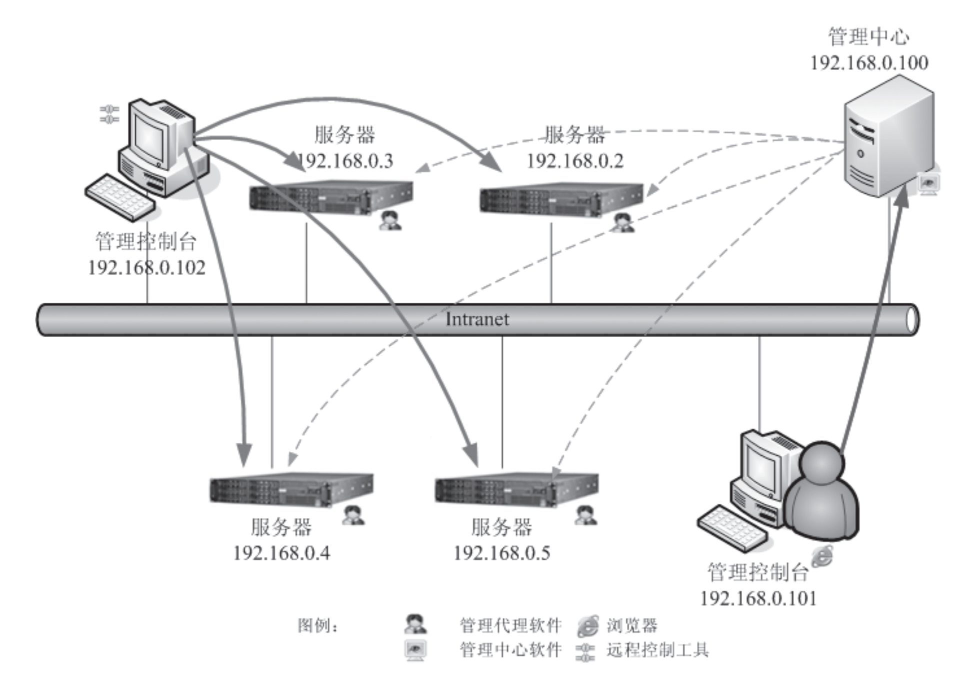
此时，用户可以将管理代理安装在被管理服务器上，将管理中心安装在另一台机器（管理控制台）上。部署完毕，用户在管理控制台通过浏览器登录同一机器的管理中心（输入http://localhost:8898），即可对服务器进行管理。管理控制台可以是一台普通PC或者笔记本电脑，也可以是另外一台服务器。

提示：特别地，用户可以将管理中心也安装在被管理的服务器上，通过使用服

务器的浏览器登录本机对该服务器进行管理，这样就构成了最为简单的单服务器管理。此时，管理员可以对服务器进行监控，但是无法在服务器关机/宕机的状态下进行管理。此外，由于管理中心占用一定的内存和 CPU 时间，可能会影响服务器上业务系统的运行。

3.2 Intranet 内多服务器集中管理

SureEyes3 用于管理 Intranet 内的多台服务器是最为典型的情况。



该场景下，管理控制台，管理中心和被管理服务器在同一个局域网内。

此时，用户需要在一台专门的机器（服务器或者高档PC）上安装管理中心。部署完毕，用户可以通过任何一个管理控制台登录到管理中心（输入 http://192.168.0.100:8898）管理局域网内所有安装了管理代理的服务器了，最多可以同时管理 128 台服务器。

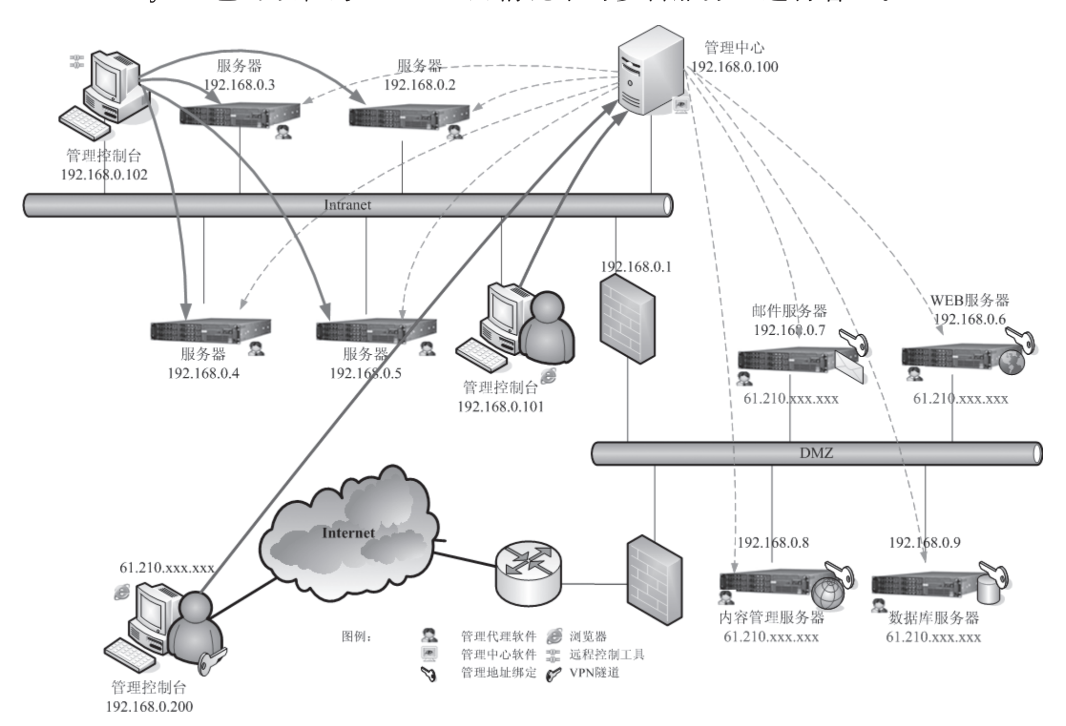
提示：不推荐用户在业务服务器上安装和运行管理中心，因为管理中心运行会

占用一定的内存和 **CPU** 时间，可能会影响服务器上业务系统的运行。

注意：远程控制工具安装在管理控制台上，不经过管理中心，可直接对服务器进行控制。

3.3 跨 Internet 的多服务器集中管理

SureEyes3 也可以在跨 Internet 的情况下对多台服务器进行管理。



该场景下，用户将企业网络划分为Intranet和DMZ区，在DMZ区中放置了邮件服务器、WEB服务器等面向Internet的应用服务器。DMZ区的每台服务器具有Intranet和Internet两个IP地址。

提示：**DMZ（Demilitarized Zone**，隔离区，非军事化区）是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立的一个非安全

系统与安全系统之间的缓冲区。这个缓冲区位于企业内部 Intranet 网络和外部 Internet 网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。在现代企业网络中，DMZ 设置是十分常见的。

此时，管理中心安装在 Intranet 内部一台专门的服务器上，管理员可以通过内部 Intranet 或者通过 Internet 登录管理中心对 Intranet 内的服务器和 DMZ 区的服务器进行集中管理。

在为DMZ区中的服务器安装管理代理的时候，用户需要配置代理确保将管理代理 IP 地址绑定到 Intranet IP 地址上（例如 WEB 服务器的管理代理绑定 IP 到 192.168.0.6 上）。具体的配置方法参见 5.2.1.3*Windows 下的管理代理配置*和 5.2.2.1*Linux 下的管理代理配置*。

同时，为了确保管理中心能够和DMZ区中的服务器进行通信，确保正确配置了 Intranet 防火墙，允许管理中心和 DMZ 区中的服务器通过代理通信端口（默认是 8688 UDP 端口）通信。

用户可以在 Intranet 内部通过管理控制台登录管理中心，进行服务器管理。如果用户希望通过Internet管理控制台登录管理中心，建议在管理控制台上启用VPN 获得 Intranet 内部 IP 访问管理中心。

提示：出于安全性考虑，在一般情况下不建议用户将管理中心部署在Internet上。

提示：不推荐用户在业务服务器上安装和运行管理中心，因为管理中心运行会占用一定的内存和 CPU 时间，可能会影响服务器上业务系统的运行。

注意：远程控制工具不经过管理中心，直接对服务器进行控制。

提示：远程控制工具和浏览器可以在管理控制台上。

第四章 安装与卸载

4.1 安装管理中心

进行管理中心的安装需要先满足以下的安装条件：

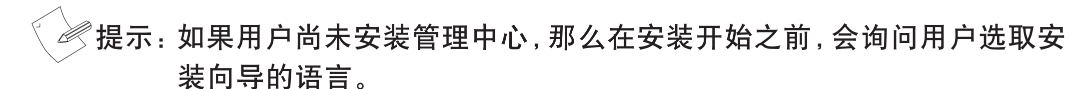
- 操作系统为下列之一：Windows2000，WindowsXP，Windows2003
- 至少 800M 的硬盘磁盘空间
- 至少 512M 内存

以系统管理员的身份登陆进行安装操作。否则安装程序会进行警告。

注意：安装管理中心本身不会占用超过200M的磁盘空间，但是存储历史信息的数据文件可能会占用600M_1G不等的磁盘空间，视用户对7.7 *历史信息存储功能*的使用情况而定。

插入Sureeyes3光盘，安装程序自动运行，选择“安装管理中心”；或者运行位于安装光盘manager目录下的SureEyes3-Manager-xxxxxx.exe，进行管理中心的安装。其中 xxxxxx 表示该软件发布的版本。

管理中心默认安装在操作系统所在驱动器的 Program Files\Lenovo\SureEyes Manager 目录下。



提示：如果用户尚未安装管理中心，那么在安装开始之前，会询问用户选取安装向导的语言。

提示：如果用户已经安装了管理中心，那么在安装之前，安装程序会提示用户先卸载原来的管理中心。推荐用户先通过控制面板卸载原有的管理中心再安装。

安装完毕，弹出管理中心配置窗口，用户可以对管理中心进行配置。如果用户修改了默认配置，那么系统会提示用户是否启动管理中心。如果没有修改任何配置，则需要用户自行从Windows托盘区中通过管理中心托盘程序启动管理中心，参见 5.3.1.2 *管理中心的运行和停止*。

安装完成后，管理中心会以 Windows 服务的形式在每次开机后自动运行。在

Windows 的服务管理中，会看到名称为“Lenovo SureEye 3 Manager”的服务。

提示：在管理中心进行带外管理的时候，系统中还会自动注册一个名称为“Lenovo SureEyes3 OOB Proxy”的服务。如果停止带外管理，则该服务会自动注销。

安装完毕，系统会在开始菜单的“程序”中增加“万全慧眼 3”目录。

4.2 安装管理代理

4.2.1 安装 Window 下的管理代理

进行 Windows 下管理代理的安装需要先满足以下的安装条件：

- 操作系统为 Windows2000，WindowsXP，Windows2003
- 至少 200M 的硬盘磁盘空间

以系统管理员的身份登陆进行安装操作。否则安装程序会进行警告。

插入 Sureeyes3 光盘，安装程序自动运行，选择“安装管理代理”；或者运行位于安装光盘 agent 目录下的 SureEyes3-Agent-xxxxxx.exe，进行管理代理的安装。其中 xxxxxx 表示该软件发布的版本。

管理代理默认安装在系统所在驱动器的Program Files\Lenovo\SureEyes Agent 目录下。

提示：如果用户尚未安装管理代理，那么在安装开始之前，会询问用户选取安装向导的语言。

提示：如果用户已经安装了管理代理，那么在安装之前，安装程序会提示用户先卸载原来的管理代理。推荐用户先通过控制面板卸载原有的管理代理再安装。

安装的过程中，用户根据服务器的实际情况选择是否安装BMC 驱动版本，以及驱动针对的操作系统类型（32 位或者 64 位），也可以不安装驱动。如果不安装 BMC 驱动，用户将无法通过带内方式对硬件健康信息进行监控。

安装完毕，系统会在开始菜单的“程序”中增加“万全慧眼 3”目录。

注意：如果服务器没有 BMC 芯片，请不要安装 BMC 驱动！如果用户选择错误的驱动安装，将可能导致服务器配置出现错误，而破坏操作系统！

安装完毕，弹出管理代理配置窗口，用户可以对管理代理进行配置。如果用户修改了默认配置，那么系统会提示用户是否启动管理代理。如果用户没有修改任何配置，则需要用户自行从Windows托盘区中通过管理代理托盘程序启动管理代理，参见 5.2.1.2 *管理代理的启动和停止*。

安装完成后，管理代理会以 Windows 服务形式在每次开机后自动运行。在 Windows 的服务管理中，会看到名称为“Lenovo SureEye 3 Agent”的服务。

安装完毕，系统会在开始菜单的“程序”中增加“万全慧眼 3”目录。

4.2.2 安装 Linux 下的管理代理

万全慧眼服务器管理代理在 Linux 下的安装包分为 sureeyesagentd-3-2.4.X.X.i386.rpm 和 sureeyesagentd-3-2.6.X.X.i386.rpm 两个软件包，分别对应 2.4 内核和 2.6 内核的两个版本的操作系统。其中 X.X 表示该软件发布的版本。安装包位于安装光盘 agent 目录下。

安装步骤如下：

首先，确保系统没有安装 sureeyesagentd 软件，可以通过以下命令查看安装的 sureeyesagentd 软件包的版本信息：

```
# rpm -q sureeyesagentd
```

如果存在其他版本的管理代理，可以通过以下命令

```
# rpm -e sureeyesagentd
```

卸载其他版本的 sureeyesagentd。

然后，安装软件，进入安装包所在的目录，使用以下命令进行安装：

rpm -ivh sureeyesagentd-3-2.4-XX.i386.rpm（用于内核版本为 2.4 的 Linux）

或者

rpm -ivh sureeyesagentd-3-2.6-XX.i386.rpm（用于内核版本为 2.6 的 Linux）

注意：可以使用 uname -a 命令查看内核版本。

如果安装成功，终端会打印出如下信息：

```
[root@redhat-as4 i386]# rpm -ivh sureeyesagentd-3.0-2.6.1.0.i386.rpm
Preparing...                ########################################### [100%]
   1:sureeyesagentd         ########################################### [100%]
Please wait...
Install sureeyesagentd success!
Starting sureeyesagentd: [  OK  ]
```

检查安装是否成功，打开进程列表，查看 sureeyesagentd 进程是否已经启动。

4.3 安装远程控制工具

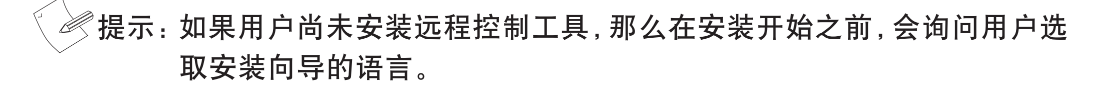
进行远程控制工具的安装需要先满足以下的安装条件：

- 待控制的服务器具有 BMC 芯片
- 操作系统为 Windows2000，WindowsXP，Windows2003
- 至少 10M 的硬盘磁盘空间

以系统管理员的身份登陆进行安装操作。否则安装程序会进行警告。

插入Sureeyes3光盘，选择“安装远程工具”；或者运行位于安装光盘RCUtility目录下的 SureEyes3-RCUtility-xxxxxx.exe，进行远程控制工具的安装。其中 xxxxxx 表示该软件发布的版本。

远程控制工具默认安装在系统所在驱动器的 Program Files\Lenovo\SureEyes RCUtility 目录下。



提示：如果用户尚未安装远程控制工具，那么在安装开始之前，会询问用户选取安装向导的语言。

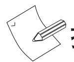
提示：如果用户已经安装了远程控制工具，那么在安装之前，安装程序会提示用户先卸载原来的远程控制工具。推荐用户先通过控制面板卸载原有的远程控制工具再安装。

安装完毕，系统会在开始菜单的“程序”中增加“万全慧眼 3”目录。

4.4 卸载管理中心

用户可以从“控制面板”的“添加删除程序”中找到“万全慧眼3管理中心”进行卸载。

卸载管理中心时，系统会提示是否删除安装目录下数据库及历史记录文件，如果用户希望保留数据库和历史记录，可以选择否。



提示：再次安装管理中心时，如果安装在之前保留了数据库和历史记录，并且安装在同一目录下面，那么安装程序会加载保留的数据库和历史记录进行安装。这样，安装完毕，用户可以继续使用原来的服务器管理信息。

4.5 卸载管理代理

4.5.1 卸载 Window 下的管理代理

用户可以从“控制面板”的“添加删除程序”中找到“万全慧眼3管理代理”进行卸载。

4.5.2 卸载 Linux 下的管理代理

使用以下命令卸载：

rpm -e sureeyesagentd

卸载完毕，控制显示卸载成功。

```
[root@redhat-as4 ~]# rpm -e sureeyesagentd
Stopping sureeyesagentd: [  OK  ]
Uninstall sureeyesagentd success!
```

4.6 卸载远程控制工具

用户可以从“控制面板”的“添加删除程序”中找到“万全慧眼3远程控制工具”进行卸载。

第五章 配置

5.1 基本概念

一般地，用户在安装完毕管理中心和管理代理之后，不必进行配置，使用系统默认的参数就能够正常使用服务器带内管理的所有功能。

但为了更有效和安全地进行服务器管理，推荐用户进行合理的配置。

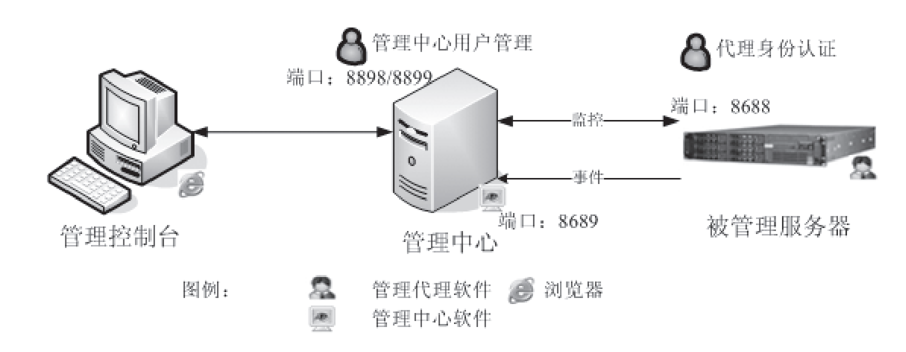
对于带内管理而言，管理中心和管理代理的配置项主要包括：服务和管理端口，认证账号和口令，通信密钥。

- 服务端口：需要配置管理中心的WEB服务的访问端口，默认是8898（HTTP）和8899（HTTPS）。
- 管理端口：管理中心接收服务器事件的端口，默认是8689；管理代理的管理端口，默认是8688。管理中心和管理代理都需要配置，并保持一致。
- 认证账号和口令：管理代理的授权管理账号口令，用于接受管理中心的管理。这个认证账号和口令就是带内管理账号和口令。

注意：管理代理的授权账号口令和管理中心用户管理中的账号口令是两个完全不同的概念。管理代理的授权账号用于控制管理中心对服务器的管理授权，而管理中心的用户账号用于控制管理员通过浏览器使用万全慧眼系统的授权。

- 通信密钥：管理代理和管理中心之间保密通信的密钥。管理中心和管理代理都需要配置，并保持一致。
- 其它配置：主要是管理代理的一些配置。包括事件接收地址设置、管理IP绑定。

如下图所示，说明了SureEyes3的基本配置内容。



对于带外管理而言，需要首先通过BMC配置工具对被管理服务器进行适当的配置，使能带外管理功能。

5.2 服务器管理代理配置

5.2.1 Window 下的配置

5.2.1.1 代理配置程序

管理代理安装的过程中，缺省情况下会勾选“立即配置管理代理”。这样安装代理完毕会运行代理配置程序，并在Windows的系统通知区生成一个托盘图标，同时显示代理的状态：



表示代理正在运行中；

表示代理已经停止运行。

双击此托盘图标可以对管理代理参数进行配置。

如果用户以后重新启动服务器，管理代理服务及其配置程序会自动运行。用户也可以从“开始”菜单的“万全慧眼3”目录下运行“配置管理代理”，启动此配置程序。

如果需要关闭代理配置程序，请在联想万全慧眼系统管理代理托盘上单击右键，在菜单中选择“退出”。

注意：退出仅仅表示退出配置程序，管理代理程序的运行不受影响。

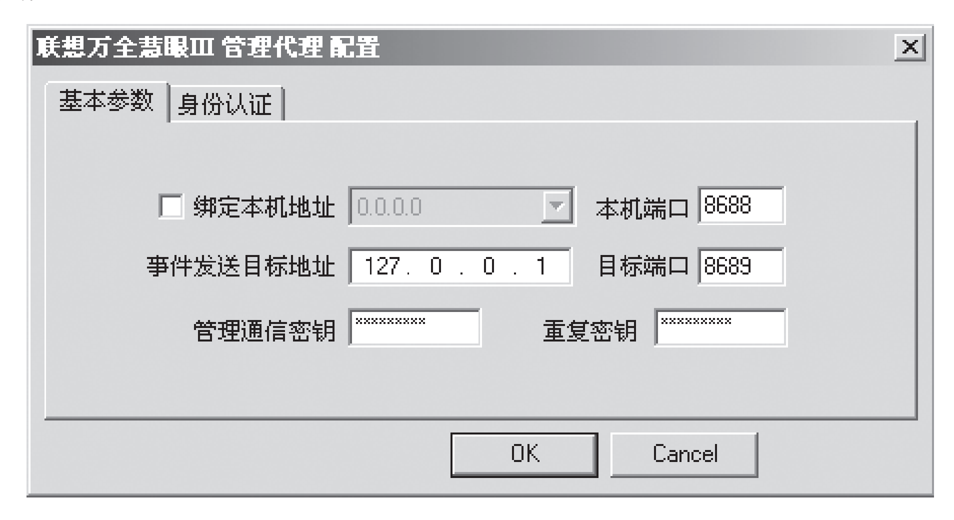
5.2.1.2 管理代理的启动和停止

如果管理代理没有启动，请在联想万全慧眼系统管理代理托盘上单击右键，在菜单中选择“启动”。代理程序将启动。

如果需要停止代理程序的运行，请在联想万全慧眼系统管理代理托盘上单击右键，在菜单中选择“停止”。代理程序将停止运行。

5.2.1.3 配置基本参数

用户双击联想万全慧眼系统管理代理托盘，或者在托盘图标上单击右键，在菜单中选择“配置”，系统将弹出联想万全慧眼系统管理代理配置对话框，显示“基本参数”。



1) 绑定本机地址：使代理程序运行在某个指定的本地地址上。这种情况下，如果服务器配置了多个IP地址，代理程序将只处理这个IP地址上接收到的请求，而忽略其他IP地址上接收到的请求；同时，也将会以这个IP地址作为发送报警事件的IP地址。如果选择不绑定，代理程序将处理服务器上全部IP地址接收到的请求，同时自动选择一个适当的IP地址，作为发送报警事件的源IP地址。
   - 一般情况下，请选择服务器上一个连接在管理网络上的IP地址作为绑定本机地址。如果没有专门的管理网络，可以选择一个用于管理的IP地址，作为代理的绑定地址。

- 如果要设置一个绑定地址，请选中“绑定本机地址”选择框，并在下拉框中选择一个本机的 IP 地址。
- 如果要取消绑定功能，请取消“绑定本地地址”选择。

2) 本机端口：管理代理程序接收请求的端口号。该端口号需要与管理中心配置的“代理配置”选项卡中的 5.3.1.3 *代理通信端口号*一致。
3) 事件发送目标地址：代理程序发送报警事件的目标IP 地址。一般情况下，这个地址就是管理中心的地址。
4) 目标端口：代理程序发送报警事件的目标端口号。该端口号需要和管理中心配置的“代理配置”选项卡中的 5.3.1.3 *事件接收端口号*一致。
5) 管理通信密钥：代理程序和管理中心之间的通信密钥。代理程序将使用这个密钥来加密和管理中心之间通信数据。需要和管理中心的管理通信密钥一致。请在“管理通信密钥”输入框中输入通信密钥（8 到 16 个字符，不能包含空格），并在“重复密钥”中再次输入相同的密钥。

配置完成后，选择“确认”按钮（某些操作系统上可能是“OK”按钮），如果配置参数发生了变化，配置界面将提示配置界面已经修改，如果代理程序正在运行，将同时提示是否需要重新启动。

选择“是”（某些操作系统上可能是“Yes”），代理程序将使用新的配置参数重新启动。

5.2.1.4 配置认证参数

请在联想万全慧眼系统管理代理托盘上单击右键，在菜单中选择“配置”。系统将弹出联想万全慧眼系统监控版配置对话框。选择“身份认证”。



1) 读权限用户：设置读权限用户的用户名和口令。使用这个读权限用户名，管理中心能够执行服务器搜索、基本信息查看、硬件健康信息查看的操作。如果需要设置一个读权限用户，请在“读权限用户”的“用户名”输入框中输入用户名（最多16个字符，只能是字母和数字）。在“密码”输入框中输入用户密码（8到16个字符，不能包含空格），并在“重复密码”输入框中再次输入相同的密码。系统缺省的用户名是 public，密码是 public999。
2) 读写权限用户：设置读写权限用户的用户名和口令。使用这个读写权限用户名，管理中心能够执行全部的操作，包括服务器搜索、基本信息查看、硬件健康信息查看、各种阈值的设置，以及服务器控制操作。如果需要设置一个读写权限用户，请在“读写权限用户”框中选择“启用”，并在“用户名”输入框中输入用户名（最多16个字符，只能是字母和数字）。在“密码”输入框中输入用户密码（8到16个字符，不能包含空格），并在“重复密码”输入框中再次输入相同的密码。系统缺省的用户名是 sureeyes，密码是 sureeeys999。

注意：读权限用户必须存在，用户可以修改其账号名称和密码，但是不能没有！

注意：用户身份认证账号和密码是区分大小写的！

配置完成后，选择“确认”按钮（某些操作系统上可能是“OK”按钮），如果配置参数发生了变化，配置界面将提示配置界面已经修改，如果代理程序正在运行，将同时提示是否需要重新启动。

选择“是”（某些操作系统上可能是“Yes”），代理程序将使用新的配置参数重新启动。

5.2.1.5 Windows 下防火墙配置

如果管理代理所在机器的操作系统安装并启用了 Windows 防火墙，那么在使用管理代理之前需要进行必要的设置。否则，将无法正确的进行服务器搜索和服务器监控。

通过控制面板进入防火墙配置的对话框。首先确认当前是否启用了防火墙，如果没有，则不必进行配置。如果启用了，那么必须配置例外。在例外选项卡中使用“添加程序”按钮添加管理代理安装目录的 bin 子目录下的可执行程序 SureeyesAgentD.exe 到例外列表中。



提示：用户也可以通过添加允许代理的本机端口号（默认是8688端口，UDP协议）使得管理代理能够正常运行。具体操作方式参见Windows操作系统防火墙配置的帮助。

5.2.2 Linux 下的配置

5.2.2.1 管理代理的参数配置

安装并启动sureeyesagentd以后，可以对sureeyesagentd的通信端口、管理中心的 IP 地址和端口，是否开启访问控制功能、是否开启只读访问控制、是否开启读写访问控制以及只读和读写访问控制的帐号进行配置。配置命令：

service sureeyesagentd set

进入配置选项：

```
[root@redhat-as4 ~]# service sureeyesagentd set
Setting sureeyesagentd: Please input one number from the below list:
0       Display the help information;
1       Show all sureeyesagentd configuration information;
2       Change the local IP binding option;
3       Change the port of sureeyesagentd;
4       Change the management center's IP and port;
5       Change the communication encryption key;
6       Set the Read-Only access control account;
7       Set the Read-Write access control account;
97      Show version information;
98      Discard changes and exit;
99      Save changes and exit;
Notice: Press <Enter> key directly to make no change and back.
Input Your Choice: _
```

第一项，输入数字 0，打印主选项帮助信息。

第二项，输入数字 1，显示当前所有的配置项的具体配置信息。

第三项，输入数字 2，选择是否绑定本地 IP，如果需要绑定，则继续选定本地的一个 IP 进行绑定。关于绑定 IP 的含义参见 5.2.1.3*Windows 下的代理配置说明*。

第四项，输入数字 3，重新设置管理代理的端口号。代理端口号的含义参见 5.2.1.3*Windows 下的代理配置说明*。

第五项，输入数字 4，设置管理中心的 IP 地址和端口号。管理中心端口也就是管理代理事件发送的目标端口，具体的含义参见 5.2.1.3*Windows 下的代理配置说明*。

第六项，输入数字 5，修改通信密钥。通信密钥的的含义参见 5.2.1.3*Windows 下的代理配置说明*。

第七项，输入数字 6，设置只读访问控制功能，用户可以设定访问控制的用户名和口令。如果用户不输入用户名和口令，系统会给定默认的用户名为 public，默认口令 public999。

第八项，输入数字 7，设置读写访问控制功能，如果启用读写访问控制功能，需要设定访问控制的用户名和口令。如果用户不输入用户名和口令，系统会给定默认的用户名为 sureeyes，默认口令 sureeyes999。用户也可以禁用该写控制帐户。

第九项，输入数字 97，显示代理的版本和版权信息：

```
Input Your Choice: 97
        Lenovo SureEyes Agent
        Version 3.0
        Copyright (c) 2002-2006 Lenovo All Rights Reserved
```

第十项，输入数字98，放弃修改并退出设置。如果选择该选项，则上一次保存之后的所有修改都不保存，并且退出设置。

第十一项，输入数字99，保存配置，并且退出设置。成功保存并退出配置后，会弹出如下提示：

```
Input Your Choice: 99
Save Changes And Exit Success!
The changes will take effect after the sureeyesagentd restarted.
Restart the agent now (y/n)?: _
```

为了使本次的设置生效，必须重新启动代理，如果用户输入"y"，并回车，则会自动重启代理。用户也可以输入"n"或者直接回车，不立即重启代理，而是自行手工重启。



提示：如果用户在修改配置后不重启代理，那么新的配置将不会生效。

提示：用户在进入设置子项后，如果用户直接回车，则放弃修改该配置选项。

5.2.2.2 管理代理的启动和停止

启动代理服务的命令：service sureeyesagentd start

停止代理服务的命令：service sureeyesagentd stop

5.2.2.3 配置命令汇总

启动代理服务：service sureeyesagentd start

停止代理服务：service sureeyesagentd stop

重启代理服务：service sureeyesagentd restart

设置代理服务：service sureeyesagentd set

获得代理服务当前状态：service sureeyesagentd status

5.2.2.4 Linux 下防火墙配置

如果管理代理所在机器的操作系统安装并启用了防火墙，那么在使用管理代理之前需要进行必要的设置，否则管理中心将无法连接管理代理。

如果在命令行模式下，用户可以输入命令lokkit或system-config-securitylevel或redhat-config-securitylevel进入防火墙配置界面。如果在图形界面模式下，用户可以通过开始菜单的“系统设置”－“安全级别”选项进入“安全级别设置”界面。如果防火墙的安全级别为Disable，那么说明没有启用防火墙，不必配置。如果安全级别为Enable，那么需要配置防火墙规则。选择定制按钮，进入定制防火墙规则的页面。

首先，在信任设备列表中选择一块活动网卡，确保该网卡上具有管理代理的管理 IP。如果用户在管理代理中选择了绑定 IP，那么该 IP 必须在此网卡上；如果用户没有绑定 IP，那么该活动网卡的 IP 必须是管理中心设定的该服务器的带内管理 IP。

然后，在其他端口中添加代理端口，格式为：端口号:udp。其中端口号是管理代理的端口号，默认为 8688。

5.3 管理中心配置

5.3.1 基本配置

5.3.1.1 管理中心配置程序

管理中心安装过程中，缺省情况下会勾选“立即配置管理中心”。这样管理中心安装完毕，配置程序会自动运行，并在 Windows 的系统通知区生成一个托盘图标。双击此图标或者通过鼠标右键并选择“配置”菜单，可对管理中心参数进行配置；通过鼠标右键选择“退出”可以退出配置程序。

用户以后重启计算机，管理中心服务及其配置程序会自动运行。用户也可以从“开始”菜单的“万全慧眼 3”目录下运行“配置管理中心”，启动此配置程序。

注意：退出仅仅表示退出配置程序，管理中心程序的运行不受影响。如果用户希望能够配置管理中心，可以从“开始”菜单的“万全慧眼 3”目录下运行“配置管理中心”。

5.3.1.2 管理中心的运行和停止

用户可以通过配置菜单来启动和停止管理中心服务。系统托盘区的图标会自动显示当前管理中心服务的状态：

表示此时管理中心服务为启动状态。

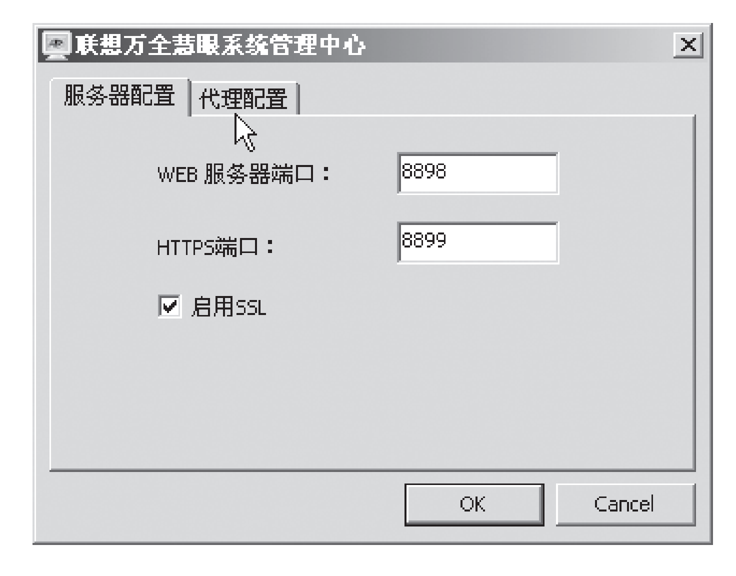
表示此时管理中心服务为停止状态。

在配置菜单中选择“启动服务”或“停止服务”后，系统将会将出现一个进度对话框，显示当前用户操作的执行进度。

5.3.1.3 配置管理中心参数

用户通过鼠标右键可以看到配置菜单，在配置菜单选择“配置管理”选项，将进入配置界面。

首先，用户可以进行“服务器配置”。



在“WEB 服务器端口”和“HTTPS 端口”，输入端口号数值，该数值必须在 0 － 65535 之间。

注意：系统默认的“WEB服务器端口”是8898，默认的“HTTPS端口”是8899。默认情况下SSL启用。

如果使用默认配置，用户可以通过在浏览器地址栏输入http://localhost:8898或者https://localhost:8899访问SureEyes3。

通过修改“启用SSL”来启用/关闭SSL服务。默认的，系统启用SSL，以获得最大限度的通信安全。

然后，用户可选择“代理配置”，进入“代理配置”界面：

联想万全慧眼系统管理中心

服务器配置 | 代理配置

代理通信端口：8688

事件接收端口：8689

管理代理通信密钥：●●●●●●●●●●●●●

密钥确认：●●●●●●●●●●●●●

OK　Cancel

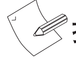
在“代理通信端口”和“事件接收端口”，输入端口号数值，该数值必须在0－65535之间。默认的“代理通信端口”是8688；默认的“事件接收端口”是8689。

注意：端口设置必须和被管理服务器的管理代理配置保持一致，否则将无法进行带内管理，详情参见5.2.1.3 *管理代理配置*。

在“管理代理通信密钥”中，输入8－16位通信密钥，密钥是除空格以外的任何其他字符。默认密钥是“sureeyes3”。

注意：密钥必须和被管理服务器端保持一致，否则将无法进行带内管理。参见

5.2.1.3 *管理代理配置*。



提示：如果一个管理中心管理2台以上的服务器，那么要求这些服务器的管理代理的通信端口、通信密钥全部保持一致。如果用户希望管理中心能够收到所有被管理服务器的事件，那么要求这些服务器的管理代理的管理中心地址（事件目标地址）都指向管理中心的IP，并且都使用相同的事件发送（接收）端口。

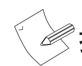
配置完成后，选择“确认”按钮（某些操作系统上可能是“OK”按钮），如果配置参数发生了变化，配置界面将提示配置参数已经修改，如果管理中心正在运行，将同时提示是否需要重新启动。

选择“是”（某些操作系统上可能是“Yes”），管理中心将使用新的配置参数重新启动。

5.3.1.4 Windows 下防火墙配置

如果管理中心所在机器的操作系统安装并启用了Windows防火墙，那么在使用管理中心之前需要进行必要的设置。否则，管理中心将可能无法接收来自服务器的事件。

通过控制面板进入操作系统防火墙配置的对话框。首先确认当前是否启用了防火墙，如果没有，则不必进行配置。如果启用了，那么必须配置“例外”选项卡的内容。在“例外”选项卡中使用“添加程序”按钮，添加管理中心安装目录的bin子目录下的可执行程序SureEyes3.exe到例外列表中。



提示：用户也可以通过添加允许事件接收端口号（默认是8689端口，UDP协议）使得管理代理能够正常运行。具体操作方式参见Windows操作系统防火墙配置的帮助。

5.3.2 高级配置

高级配置是指管理员无法通过管理中心修改的参数，需要用户手工编辑管理中心的配置文件。

管理中心可以配置的高级参数包括：信息存储参数、服务器存活检查服务参数、事件记录清除服务参数。

5.3.2.1 信息存储参数配置

信息存储服务是提供给用户可以指定存储某服务器历史信息(进程信息)的功能，管理员可以根据实际情况，配置存储的采样时间、导出存储数据的时间跨度、同时存储信息的服务器数量限制、存储信息文件的保存路径。

信息存储的配置参数保存在Sureeyes3安装目录（下称SUREEYES_HOME）/sureeyes/conf/scheduler.properties 文件中。以下为配置文件缺省情况下的配置：

frequency=2000

配置存储的采样时间，每隔采样时间便会实时获取一次监视数据的值并保存。单位为毫秒，缺省值为 2000，即每 2 秒采样一次。

limit=10

同时存储信息的服务器数量限制,管理中心在同一时间最多允许此数量限制的服务器进行信息存储。设置这样的限制主要是考虑到服务器的性能。单位为台，缺省值为 10，即缺省情况下最多可以设置 10 台服务器存储信息。

path=

存储信息文件的保存路径。缺省情况下，所有的存储数据文件都存放在SUREEYES_HOME/history下，根据实际情况和需要可以自行调整。自行配置时，直接填写希望存放文件的绝对路径即可，如 C:/history/（使用 Unix 样式分隔符）。

5.3.2.2 服务器存活检查服务参数配置

服务器存活检查服务是针对已经搜索到的但没有添加到被管理列表中的服务器进行的。对于这些服务器，将根据服务器存活检查服务器参数定期重新尝试搜索，如果服务器已经不存在或发现时间过长（二者满足其一即可)，则将其从搜索结果中移除。管理员可以根据实际情况，配置服务每次启动的时间、服务启动的频率、重新尝试搜索的重试次数、过期时间。

服务器存活检查服务的配置参数存放在 SUREEYES_HOME/sureeyes/conf/survival.properties 文件中。以下为配置文件相关部分的缺省情况下的配置：

startat=3:00:00

服务每次启动的时间，服务启动的准确时间。格式为24小时制标准时间格式，即 HH:mm:ss，必须填写完整。缺省值为 3:00:00，即凌晨 3 点启动服务。

提示：建议尽量将服务的启动时间调整到网络状况比较畅通时进行，以提高效率。

frequency=1

服务启动的频率，服务每隔启动频率时间运行一次。单位为天，缺省值为1，即每天运行一次。

detecttimes=1

重新尝试搜索的重试次数，重新搜索时搜索重试次数，如果每次均未搜索到服务器，则认为服务器已不存在。单位为次，缺省值为1，即只搜索1次，如果发现即判断存活，如果未发现即判断不存在。

expired=2

过期时间，当发现服务器的时间距当前时间超过过期时间则也认为该服务器需要移除。单位为天，缺省值为2，即如果发现服务器的时间超过2天则无论该服务器还是否存活，都将会被从搜索结果中移除。

5.3.2.3 事件记录清除服务参数配置

事件记录清除服务是指系统根据用户在系统配置管理中设定的13.4*事件记录保存策略*，定期地对保存在管理中心的事件记录进行清理的服务。管理员可以根据实际情况，配置服务的启动时间。

事件记录清除服务的配置参数存放在SUREEYE_HOME/sureeyes/conf/survival.properties文件中。

以下为配置文件相关部分的缺省情况下的配置：

eventlogcheckpoint=4:10:00

服务启动时间，服务启动的准确时间。格式为24小时制标准时间格式，即HH:mm:ss，必须填写完整。缺省值为4:10:00，即凌晨4点10分启动服务。

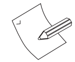
提示：建议尽量将服务的启动时间调整到管理中心所在主机访问量较小的时候进行，以提高效率。

5.4 管理员浏览器的配置

一般情况下，管理员使用IE6以上或者Firefox1.5以上版本的浏览器就能够登录和访问管理中心了。

从IE6开始，为了增强浏览器的安全性，Microsoft为IE设置了许多安全参数。为了能够正常使用IE访问管理中心，用户必须进行必要的设置。

用户需要确认当前访问的管理中心URL在浏览器设定的“本地Intranet”或者“受信任的站点”区域之内。用户可以在登录管理中心之后，查看浏览器下面的状态栏右侧可以知道当前URL所在的安全区域。如果此时不在上述安全区域内，需要手工将管理中心URL添加到上述安全区域内。具体的添加方法参见IE的使用说明。



提示：用户可以双击浏览器右下角的安全区域，进入Internet安全性设置；或者打开IE的帮助页面，搜索“安全区域”获得关于安全区域的帮助。

5.5 BMC配置

注意：使用BMC配置工具之前，请确认待配置的服务器具有BMC芯片！

用户在使用带外管理方式进行服务器管理之前，需要先进行BMC配置。用户也可以通过BMC配置工具随时修改带外管理的参数。基本的配置内容包括：带外管理的IP地址、子网掩码和网关、带外管理的密码。更为具体的BMC配置工具的使用方法参见16BMC配置。

5.5.1 BMC出厂设置

联想的服务器在出厂前，已经为BMC设备设置很多初始值。具体信息如下：

1. 网卡1网络配置

网卡1的带外IP地址：192.168.0.2

网卡1的带外网关地址：0.0.0.0

网卡1的带外子网掩码：255.255.255.0

网卡1的带外网络类型：Static类型，表示通过BMC配置工具来配置IP信息

提示：以上信息用户可以通过 bmccfg 工具获得，具体操作如下：在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入
bmcc0fg> get -t network 1
其中 1 是阿拉伯数字，表示网卡 ID 号。

2. 网卡 1SOL 配置

网卡 1 是否支持 SOL 功能：Enable
网卡 1SOL 的数据传输率：19.2kbps

提示：以上信息用户可以通过 bmccfg 工具获得，具体操作如下：在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入
bmccfg> get -t sol 1
其中 1 是阿拉伯数字，表示网卡 ID 号。

3. 网卡 2 网络配置

网卡 2 的带外 IP 地址：192.168.0.3
网卡 2 的带外网关地址：0.0.0.0
网卡 2 的带外子网掩码：255.255.255.0
网卡 2 的带外网络类型：Static 类型，表示通过 BMC 配置工具来配置 IP 信息

提示：以上信息用户可以通过 bmccfg 工具获得，具体操作如下：在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入
bmccfg> get -t network 2
其中 2 是阿拉伯数字，表示网卡 ID 号。

4. 网卡 2 的 SOL 配置

网卡二是否支持 SOL 功能：Enable
网卡二 SOL 的数据传输率：19.2kbps

提示：以上信息用户可以通过 bmccfg 工具获得，具体操作如下：在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入
bmccfg> get -t sol 2
其中 2 是阿拉伯数字，表示网卡 ID 号。

5. BMC 用户访问密码

BMC 用户访问密码：lenovo

5.5.2 设置 BMC

第一次使用BMC设备前，用户只需要设定一块网卡的带外配置，即可将服务器接入网络使用，并且可以通过SureEyes3进行BMC管理（带外管理）。具体操作如下：

1. 设置 BMC 网络 IP 地址

在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入

bmccfg> set -t network 1 ip XX.XX.XX.XX

“XX”表示为 10 进制的数字，每一个数字在 0~255 之间。

2. BMC 网关地址

在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入

bmccfg> set -t network 1 gateway XX.XX.XX.XX

“XX”表示为 10 进制的数字，每一个数字在 0~255 之间。

3. BMC 子网掩码地址

在 DOS 环境下，运行 bmccfg 工具，屏幕出现 bmccfg> 提示符后，键入

bmccfg> set -t network 1 subnet XX.XX.XX.XX

“XX”表示为 10 进制的数字，每一个数字在 0~255 之间。

在设置了BMC网络IP地址、BMC网关地址和BMC掩码地址后，用户就可以通过 BMC 设备对服务器进行管理了。

第六章 功能概述

6.1 主界面

系统主界面如下图所示：



标题区：显示软件的标识Logo，并提供基本操作功能按钮。

- 首页：使主操作区恢复为如上图所示的服务器管理页面；
- 刷新：单独刷新主操作区；
- 帮助：显示帮助窗口；
- 退出：退出本系统，如要再次使用必须重新登录。

功能节点区：显示软件所能提供的所有功能的选择菜单，可以通过点击不同的节点查看不同的功能页面。当进入服务器监控状态时，功能节点区将自动切换为单机监控功能节点状态。

主操作区：在该区域中显示软件的主要内容，并可进行各种操作。

状态栏：显示软件当前的活动状态。状态包括是否接受到新的事件、是否发现了新的服务器以及当前登录的用户名称。用户可以点击当前登录的用户名称上的链接来修改自己的帐号信息。

6.2 基本功能

6.2.1 服务器管理

服务器管理以列表的形式显示出当前可以被控制监视的所有服务器。管理视图不仅提供直观地设备运行状况概览，而且选择每台服务器，管理员可以进入该服务器的监控界面，进行细致的管理。



在列表中可以直观的显示出服务器的名称、类型、操作系统、状态等等信息。

用户可以对被管理的服务器进行分组。通过将服务器放在各个不同的组中，极大地提高管理效率。默认地，所有服务器都被放在“未分组服务器”组中。

具体请参见 7 *服务器组织管理*。

6.2.2 服务器监视和控制

通过选择服务器管理视图中服务器列表中的某台服务器，可以进入该服务器监视和控制界面。



当进入服务器监控界面后，功能节点区也会自动进入单服务器监控功能节点状态。通过选择这些不同的节点，可以查看到相应的实时监视数据，并对服务器实施各种控制操作。

具体请参见 7.7.2 *服务器监控管理*。

6.2.3 服务器事件管理

通过选择系统管理视图中的事件管理，可以进入全局的事件管理界面，查看所有被管理服务器发生的事件列表。默认地，按照事件的接收时间进行倒排序，即最后发生的事件排在前面。

您的位置：事件管理

导出Excel格式　导出CSV格式

☐ 只显示未恢复的事件

☐ 时间过滤

	服务器名称 全部	事件类型 全部	部件 全部	事件等级 全部	事件接收时间	描述	确认人 全部	明细
☐	soc	性能事件	CPU	普通事件	2006-06-24 14:55:56	当前CPU利用率为33%,恢复正常	? 确认	
☐	soc	性能事件	CPU	警告事件	2006-06-24 14:55:51	当前CPU利用率为86%,高于设定为80%的安全上限,仍然低于告警上限	? 确认	
☐	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:46:36	盘符为I的IDE硬盘插入服务器	? 确认	
☐	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:27:41	盘符为G的逻辑分区被创建	? 确认	
☐	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:27:41	盘符为G的逻辑分区被删除	? 确认	
☐	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:26:01	盘符为G的未知磁盘设备插入服务器	? 确认	
☐	soc	性能事件	CPU	普通事件	2006-06-23 20:47:28	当前CPU利用率为15%,恢复正常	? 确认	
☐	soc	性能事件	CPU	严重事件	2006-06-23 20:47:18	当前CPU利用率为100%,高于设定为90%的告警上限	? 确认	
☐	soc	性能事件	CPU	普通事件	2006-06-23 20:46:57	当前CPU利用率为6%,恢复正常	? 确认	

通过点击系统管理视图中的服务器管理,可以在显示的服务器列表中选择被管理服务器,然后点击服务器名称可以进入单服务器的管理页面。当进入单服务器管理界面，点击导航栏左端的事件管理，可查看所有这台服务器所发生的事件信息。

提示：在全局事件管理列表中,如果有多个主机的服务器名称相同。可以通过鼠标指针悬浮于服务器名称之上看到其带内管理 IP，和带外管理 IP。

具体请参见 9 *服务器事件管理*。

6.2.4 服务器带外管理

如果服务器当前没有启动操作系统,或者没有安装管理代理,用户仍然可以借助带外管理功能对服务器进行监控。

SureEyes3带外管理功能能够监视具有BMC芯片的服务器的BMC信息和硬件健康信息，并可以对服务器进行设备ID灯控制、远程开机，远程关机、远程重启、前面板接管、SEL 清除等控制。

具体请参见 8.4.3 *服务器硬件健康信息监视*和 8.5.2 *服务器控制*。

6.2.5 服务器远程控制

对于具有 BMC 芯片的服务器，通过 SureEyes3 的远程控制工具，管理员可以将本地IDE设备虚拟成远程服务器的IDE设备，并通过IPMIv2.0定义的SOL（Serial over LAN）功能远程接管服务器的开机过程，使用户有机会进行远程的服务器诊断和修复。

具体请参见 15 *服务器远程控制工具*。

第七章 服务器组织管理

7.1 功能简介

服务器组织管理包括服务器信息管理、增加和删除服务器、创建/编辑服务器组、删除服务器组、服务器搜索等。

在服务器列表中，显示了每台服务器的名称、类型、操作系统、当前运行状态、地址等基本信息。

管理员可以通过点击功能按钮增加和删除服务器。

在管理视图中，可以创建服务器组以便于管理，创建后也可以重新编辑服务器组、删除该服务器组。

管理员可以通过 IP 地址或网段来搜索服务器。

7.2 界面概述

登录 SureEyes3，点击“全部展开”，看到如下界面：



在上图中可以看到每台服务器的基本信息，并显示功能按钮“历史信息”、“明

细”、“删除”、“全选”、“重置状态”等。如果您创建了服务器组，还将看到"移动"按钮。在界面右上角，您还能看到“服务器搜索”、“新增组”按钮。

对于发生了事件的服务器，还会在服务器的左侧出现一个事件提示图标。

提示：事件提示图标和“重置状态”的使用说明参见 9 *事件管理*的 9.7 *事件告警*。

7.3 基本操作

登录 SureEyes3，点击“全部展开”按钮，看到服务器管理列表，显示出当前所有被管服务器。点击“全部收拢”，列表则会自动收缩。

点击服务组名称前的图标“ ”，可以看到该服务器组所有被管理服务器，同时图标“ ”变为“ ”，点击服务器组名称前的图标“ ”，将收拢该组管理列表，同时图标“ ”变为“ ”。

管理员可以点击右上角的“服务器搜索”，来发现新的服务器；用户和管理员都可以点击右上角的“新增组”，创建新的服务器组，以便于将被管服务器分类。

7.4 服务器搜索

1. 搜索服务器

管理员第一次登录到系统后，首先要搜索新的服务器。只有管理员有搜索服务器的权限，普通用户没有。

点击“服务器搜索”，看到“新发现服务器列表”和“可更新服务器列表”，点击右上角的“新搜索”，弹出“服务器搜索”窗口。

填写 IP 地址范围的时候，也可以只填写“开始”或“结束”，则只对该 IP 地址进行搜索。

点击“可供参考的历史搜索范围”下拉列表，可以看到最近的十次搜索范围和本地搜索选项。

填写完毕 IP 地址范围，点击“开始搜索”，即可进行服务器搜索。如果有其他人正在搜索，系统提示“其他人正在搜索中，请等待”。

提示：用户在选择搜索范围的时候，尽量事先了解网络中有效IP地址的分布，如果用户选择的搜索范围太大，而这个范围内有效的IP又很少，搜索时间可能会较长，从而导致其他用户无法及时的进行搜索。

提示：相同服务器判定原则：如果一台服务器具有多个带内IP地址，那么服务器搜索会自动认为这些IP地址对应同一台服务器。如果服务器的带内IP地址发生了变更，那么如果按照新的带内IP地址进行搜索，系统会自动将那台服务器标记为待更新服务器。如果一台服务器同时具有带内IP和带外IP，那么对于Windows服务器，系统会自动将其对应为同一台服务器；对于Linux服务器，系统则会认定为两台服务器。对于Linux服务器，如果用户需要同时具有带内管理和带外管理功能，需要先进行带内或者带外搜索，并添加到管理列表中，然后再编辑服务器明细信息，手工添加带内或者带外IP地址。

2. 添加服务器

完成搜索后，如果该服务器是新发现的服务器，那么搜索结果出现在“新近发现的服务器列表”中。点击“添加”，弹出“添加服务器”窗口。如果用户搜索到的服务器具有带内管理IP，那么对话框提示填写带内管理帐号，带内管理密码；如果用户搜索到的服务器具有带外管理IP，那么对话框提示填写带外管理密码；如果用户搜索到的服务器同时具有带内管理IP和带外管理IP，那么对话框提示输入带内带外账号密码。点击“确定”，服务器被添加到服务器组中。默认地，被管理服务器的带内管理帐号是sureeyes，密码是sureeyes999；带外管理帐号是lenovo，密码是lenovo。

提示：带内管理帐号是指运行在被管理服务器上的管理代理设定的帐号；带外管理密码是指被管理服务器BMC的管理密码。

提示：被管理服务器的带内管理帐号口令可以通过管理代理的配置程序进行修改。分别参见5.2.1.4*windows下管理代理的配置说明*和5.2.2.1*Linux下管理代理的配置说明*。被管理服务器的带外管理密码需要使用16*BMC配置工具*进行修改。

3. 更新服务器

如果搜索的服务器已经存在于被管理服务器列表中，但是发现的方式和列表中的发现方式不同（例如，列表中服务器是带内发现，而搜索是带外发现），那么该服务器将出现在“待更新服务器列表”中。用户可以点击“更新”，对被管理服务器列表中的那台服务器信息进行更新。

提示：在更新服务器的时候，系统会提示输入带内或者带外管理账号口令，如果以前没有输入过，则必须输入，如果以前输入过，则可以不输入，表示沿用原来的账号口令。

7.5 服务器信息管理

登录 SureEyes3，点击服务器管理，可以看到各台服务器的基本信息。

以服务器 bj-office 为例，如下图所示：

服务器名称 △	服务器类型	操作系统	状态	带内管理IP	带外管理IP	历史信息	明细	删除
bj-office	Lenovo WQ R510 G6			172.100.1.24	172.100.1.108	否		✕

服务器名称为 bj-office。

服务器类型为 Lenovo WQ R510 G6。

操作系统栏显示“ ”，表示 WINDOWS 操作系统，若显示为“ ”，则表示为 LINUX 操作系统。

状态显示为“ ”，表示带内管理状态。若显示为“ ”，表示带外管理状态，若显示为“ ”，表示不可管理状态。点击状态图标，系统会立即进行状态监测，判定当前服务器状态，并设置状态图标。

提示：不可管理的含义包括：操作系统关闭，并且 BMC 没有工作；或者操作系统正常运行，但是 BMC 没有工作，而且管理代理也没有运行。

带内管理 IP 为 172.100.1.24，带外管理 IP 为 172.100.1.108；

历史信息栏为“否”，表示不存储历史进程信息。点击“否”，用户可以看到一个对话框，选择是否进行历史信息存储。

点击“明细”，可以看到服务器的更多信息：

您的位置：服务器管理>服务器明细

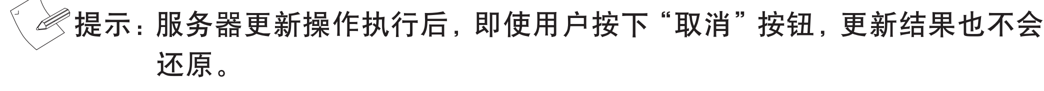
修改管理IP只会改变被管服务器在管理中心的注册IP地址，而不会改变被管服务器的IP设置。

服务器类型	Lenovo WQ R510 G6
操作系统	
状态	
带内管理IP	172.100.1.24
带外管理IP	172.100.1.108
带内管理帐号	sureeyes
带内管理密码	不填写表示不修改
带外管理密码	不填写表示不修改

基本信息	
服务器名称	bj-office
服务器型号	Lenovo WQ R510 G6
慧眼代理版本号	3.0
系统描述	Hardware : x86 Family 15 Model 6 Stepping 1 - Software : Windows Server 2003 Enterprise Edition Service Pack 1 Build 5.2.3790
主机名称	lenovo-8zztxl3w
管理员联系方式	
设备放置地点	
说明	
IPMI主版本号	2
IPMI次版本号	0
BMC的FW主版本号	0
BMC的FW次版本号	70

提交　取消　更新

其中一些信息是不能由用户更改，如服务器类型，操作系统，状态，服务器型号，慧眼代理版本号，系统描述，主机名称，BMC的FW版本号，IPMI版本。其他的信息可由用户配置。配置完成，点击“提交”系统会根据用户的设定刷新服务器的各项信息。用户也可以通过点击“更新”按钮进行服务器信息更新，系统会自动对服务器进行扫描，更新各项信息。


提示：服务器更新操作执行后，即使用户按下“取消”按钮，更新结果也不会还原。

7.6 服务器组管理

1. 新增组

系统默认只有“未分组服务器”组，用户可以创建新的组，以便于管理。

点击右上角的“新增组”按钮。在弹出的“新增组”窗口中，填写相关信息，其中“组名称”是必须填写的，也可以选中“为该组添加成员”，添加服务器到该组中。点击“确定”，“新增组”窗口关闭，可以在管理视图中看到刚刚创建的组。

2. 修改组信息

点击“组明细”，弹出“修改组”窗口，可以查看组的明细，并修改组名称和组描述。

3. 移动服务器

选中一台或多台服务器，点击“移动”，用户可以把服务器从一个服务器组移动到其它服务器组中。

4. 删除服务器

选中一台或多台服务器，点击“删除”，将弹出删除确认窗口。如果确认，选定的服务器将被删除。如果用户选择待删除的时候位于“未分组服务器”中，那么确认删除会将选定服务器彻底从管理服务器列表中删除，无法再进行监控。如果待删除的服务器位于其他组中，那么确认删除会将选定服务器移动到“未分组服务器”中去。

5. 删除组

点击“删除该组”，用户可以将自己创建的组删除，组中的服务器全都被删除到“未分组服务器”中。

“未分组服务器”组不能删除。

7.7 历史信息存储

7.7.1 基本操作

SureEyes3 提供了存储服务器进程信息功能，可以存储最近 1 小时进程信息。

1. 设置是否存储历史信息

在管理列表中，有“历史信息”栏，显示“是”或“否”，表示存储或不存历史信息，用户可以进行设置。

提示：如果用户选择否，那么表示从此刻开始，不再记录历史信息，但是原有的历史信息仍然保留。

注意：默认情况下，用户最多可以选择 10 台服务器进行历史信息存储。如需同时对更多地服务器进行历史信息存储，参见 5.3.2 *管理中心高级配置*。选择同时存储历史信息的服务器数量越多，将导致管理中心性能下降，并可能占用更多地磁盘空间！

2. 导出历史信息

点击该服务器名称对应的链接，进入单服务器监控界面，在基本信息的最下面有“历史信息导出”链接，可以导出为 Excel 或 CSV 格式。

导出的时候，必须选择时间。如选择“2006-06-01 日 12 时 30 分起 10 分钟内”，表示将要导出 2006 年 6 月 1 日 12:30 分起 10 分钟内的进程信息。点击“导出 Excel 格式”或“导出 CSV”格式，就可以导出该时段的进程信息。

注意：用户导出的文件会进行 zip 压缩处理，得到的都是 zip 压缩文件，用户需要进行解压缩得到 CSV 格式或者 Excel 格式的文件。

提示：如果某个用户正在导出一台服务器的历史信息，那么其他用户就不能对该服务器进行历史信息导出操作，系统会提示“不允许多人同时导出同一台服务器的历史信息文件，请稍候再试。”

7.7.2 分析历史信息

用户可以对导出的历史信息（进程信息）进行分析处理，帮助管理员判断最近一段时间服务器进程的运行状况，例如协助分析导致服务器宕机的原因。

导出的历史信息有csv文本文件格式和Microsoft Excel格式。文件中第一行是标题栏，第二行开始是进程记录信息。标题栏的内容包括了时间、进程名称、线程数、优先级、PID、CPU 占用率、CPU 时间、内存使用信息。

在记录进程信息的时候，先记录某个时间点的所有进程的运行快照，然后再记录下一个时间的所有进程运行快照，以此类推，最后记录 10 分钟内的所有进程的运行快照。

对于csv文本文件格式的历史信息文件，用户可以使用其它工具软件进行分析处理。对于Excel格式的历史信息文件，用户可以使用其它工具软件进行分析处理，也可以直接使用 Excel 软件进行简单的分析。

用户使用 Excel 打开历史信息文件后，选中第一行标题栏，然后选择“数据”菜单中的“筛选” – “自动筛选”，这样用户就可以对标题栏进行过滤分析了。

用户可以选择某个时间点，查看该时刻所有进程的运行状态；用户还可以选择某个进程名称，查看 10 分钟内该进程的运行变化情况。

第八章 服务器监控管理

8.1 功能简介

服务器监控主要包括了设备监视和设备控制两大部分内容。

管理员通过服务器监视的功能，可以监视服务器设备的多种信息，包括：服务器基本信息、资产信息、性能信息、健康信息。

管理员通过服务器控制的功能，远程控制服务器，包括：服务器操作系统控制、服务器电源管理、服务器远程控制（前面板控制和 ID 灯控制）、WOL 开机等。

此外，对于某些与系统性能有关的信息，用户还可以设置监控阈值。

注意：服务器监控管理的部分功能仅对具有BMC芯片的服务器有效。具体参见服务器监控管理的详细说明。

8.2 界面概述

在管理中心，通过点击服务器管理视图中任意一台安装并运行了服务器管理代理软件的服务器的名称就可以进入服务器监控页面。

进入服务器监控页面，首先显示的是服务器基本信息，如下图示：



当您点击进入服务器监控页面后，功能节点区将会变为服务器监控视图 ，以方便您的操作。您会在功能区服务器监控视图的右上角见到两个图标。点击图标就会将所有的管理节点全部展开，供您选择；点击图标就会将所有的管理节点全部收拢。

同时在主操作区将会显示当前被监控主机的基本信息。在主操作区的左上方，您将会看到当前服务器的管理路径位置及管理IP。在主操作区的中部，将会显示服务器的基本信息，其中包括服务器名称、型号、系统描述、主机名称、管理员联系方式、设备放置地点、操作系统信息、CPU信息、内存信息。如果您选择了存储服务器历史信息，那么在内存信息下方还会出现"历史信息导出"一项，以供您导出历史信息进行查看。

在服务器监视节点下，可以看到该服务器可以进行实时监控的项目信息分类，如性能信息、资产信息、硬件健康信息。通过点击这些不同分类信息下的节点，可以查看到相应项目的实时监视数据。

在监视服务器的时候，用户随时可以通过点击页面右上角的“刷新”按钮，获得最新的监视信息。

提示：SureEyes3为了提高系统响应的速度，内建了监视信息缓冲机制，因此用户在使用刷新按钮更新监视信息的时候，只是从缓冲区中更新。如果用户希望直接从服务器获取其当前监视信息，可以进入7.5*服务器信息管理*的服务器列表，点击需要更新的服务器的“明细”按钮，进入“服务器明细”对话框，点击“更新”按钮即可。

8.3 基本信息

在基本信息页面显示了该服务器的基本信息、操作系统基本信息、CPU信息和内存信息。

基本信息：是储存在管理中心的服务器基本信息，而不是实时从服务器上获取的。由于这些信息一般情况下不会发生变化，所以在搜索到服务器后管理中心即记录下这些信息，以备随时显示。这些信息会不定期的由管理中心自动与服务器进行同步，以保持基本信息的尽量接近实际情况。如果需要的话，您也可以在主页上选择要更新信息的服务器，点击服务器明细按钮，选择更新，进行手工更新。

提示：强烈建议您在更改服务器信息后进行手工更新，以保证监控信息准确无误。

操作系统基本信息：如果是 Windows 操作系统，包括类型、版本、补丁和已启动时间；如果是 Linux 操作系统，包括类型、版本和已启动时间。

CPU 信息：包括了数量、型号、是否多核、是否支持超线程。

内存：内存的总容量。

8.4 服务器监视

8.4.1 性能信息

8.4.1.1 主机性能

点击功能节点区的“服务器监视”-“性能信息”-“主机性能”选项，即可进入主机性能监控页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和 IP 信息，界面中显示了物理内存、平均 CPU 利用率、逻辑 CPU 利用率、磁盘驱动器、逻辑磁盘等信息。

- 物理内存：通过物理内存一项，您可以实时的监控被管服务器的物理内存情况。其中包括物理内存的总量和物理内存利用率信息，这一监控数据通过利用率状态条可视化表示出来。在这里还可以显示物理内存监控的利用率报警上限和安全上限。
- 平均CPU利用率：通过平均CPU利用率一项，您可以实时的监控被管服务器的平均CPU利用率信息。平均CPU利用率是指服务器上若存在多个逻辑CPU（包括多核 CPU、超线程）的时候，各个逻辑 CPU 的平均利用率。这一监控数据通过利用率状态条可视化的表现出来。还在这里还可以显示 CPU 监控的利用率报警上限和安全上限。
- 逻辑CPU利用率：这一项将更加详细的为您提供被管服务器的CPU使用信息，这里将详细的列出各个逻辑CPU的使用情况，以便您对多核CPU、超线程 CPU 进行更为细致的监控管理。
- 磁盘驱动器：在磁盘驱动器一项，您将看到被管服务器的硬盘驱动器信息，

包括驱动器的编号、容量、状态以及实时监控到的驱动器 IO 流速。

- 逻辑磁盘：在这里您可以方便的对每一个逻辑磁盘进行监控管理，您可以看到每一个逻辑磁盘的卷名、容量、已用空间、剩余空间、使用率，还可以看到各个逻辑磁盘分区的使用率报警上限和安全上限。

在主操作区的一些位置，例如“平均 CPU 利用率”后面、“物理内存”后面、“逻辑磁盘”信息的后面会显示有图标 ，说明此监视项目可以进行阈值设置，以便用户对特定的服务器性能指标进行监控。点击图标 将弹出阈值设置窗口。通过拖动滑动杆或直接输入阈值数值即可进行阈值设置，当设置完成后点击确定按钮最终确认设置，即可完成对该服务器的阈值设置，点击关闭按钮就可以在页面上看到修改后的效果。

在阈置设计界面中将会有该阈值的报警上限、安全上限、安全下限（若有）、报警下限（若有）的设置滑块。这些限制值之间的大小关系是：

报警上限≥安全上限≥安全下限（若有）≥报警下限（若有）

提示：系统将不允许以上值的大小关系更改。例如若所设安全上限大于报警上限，系统将会把所设的安全上限自动降至系统可接受的最大值，即等于报警上限的值。

提示：安装和运行在服务器上的管理代理在监视 CPU、内存和磁盘的利用率阈置的时候，如果发现连续三次检测周期都超过阈置，管理代理才认为 CPU、内存或者磁盘的利用率超过阈置。CPU 利用率阈置和内存利用率阈置检测周期为 2 秒，磁盘利用率阈置检测周期为 200 秒。

8.4.1.2 网络性能

点击功能节点区的“服务器监视”-“性能信息” -“网络性能”选项，即可进入网络性能监控页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和 IP 信息，界面中显示了网络接口数量和接口详细信息，包括接口描述、类型、接口速度、状态以及实时监控到的入流量、入流速、出流量、出流速等信息。

8.4.1.3 进程

点击功能节点区“服务器监视”-“性能信息”-“进程”选项，即可进入网络性能监控页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中实时的显示了当前被管服务器的进程信息，包括进程名称、线程数、优先级、PID、CPU占用率、CPU时间、内存使用等信息。您只需点击列表的列标题，就可以按所需要的升序、降序进行排列。



提示：对于 Linux 操作系统，没有线程数信息。

对于服务器进程信息，用户可以实时保存到历史信息中去。具体参见7.7历史信息存储。

8.4.2 资产信息

8.4.2.1 BIOS

点击功能节点区的“服务器监视”-“资产信息”-“BIOS”选项，即可进入BIOS信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器BIOS的版本号、制造商、发布日期等信息。

8.4.2.2 BMC芯片

点击功能节点区的“服务器监视”-“资产信息”-“BMC芯片”选项，即可进入BMC芯片信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器BMC芯片的设备ID、IPMI主版本号、IPMI次版本号、FW主版本号、FW次版本号等信息。下方还有BMC芯片的IP地址、子网掩码、网关、MAC地址等信息。

提示：这里显示的IP地址等网络信息都是BMC带外管理的网络信息。

注意：BMC芯片信息获取仅对具有BMC芯片的服务器有效。

8.4.2.3 CPU

点击功能节点区的“服务器监视”-“资产信息”-“CPU”选项，即可进入CPU信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的CPU型号、厂商、家族、物理CPU总个数、核总个数、逻辑CPU总个数、主频，是否支持超线程、是否多核、每个物理CPU的核数量、每个核的逻辑CPU数量。下方还显示了每个逻辑CPU的编号、所在物理CPU编号、所在核编号、当前主频等信息。

8.4.2.4 内存

点击功能节点区的“服务器监视”-“资产信息”-“内存”选项，即可进入内存信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的物理内存容量。下方还显示了每个内存插槽的索引号、插槽ID及所插内存容量信息。

8.4.2.5 磁盘驱动器

点击功能节点区的“服务器监视”-“资产信息”-“磁盘驱动器”选项，即可进入磁盘驱动器信息页面，在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的磁盘驱动器卷标、卷名、文件系统、容量以及物理磁盘信息。下方以可视化图形的方式显示了被管服务器的磁盘驱动器总体情况，包括硬盘驱动器的类型、大小、状态以及分区情况信息。

当您把鼠标放在磁盘驱动器名称上的时候，会出现悬浮框提示，向您显示这一块磁盘的一些信息，包括：磁盘的编号、型号、磁盘类型、容量、状态、控制器驱动的提供商和版本等信息。

8.4.2.6 声卡

点击功能节点区的“服务器监视”-“资产信息”-“声卡”选项，即可进入声卡信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的声卡类型和制造商信息。

8.4.2.7 显卡

点击功能节点区的“服务器监视”-“资产信息”-“显卡”选项，即可进入显卡信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的显卡型号，显存大小，水平及垂直像素，最小刷新率，当前刷新率等信息。

提示：如果被管服务器使用的是Linux/Unix家族操作系统，将不会显示显卡信息。

8.4.2.8 网络适配器

点击功能节点区的“服务器监视”-“资产信息”-“网络适配器”选项，即可进入网络适配器信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的网络适配器名称、驱动提供商、驱动版本等信息。

8.4.2.9 调制解调器

点击功能节点区的“服务器监视”-“资产信息”-“调制解调器”选项，即可进入调制解调器信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的调制解调器类型、制造商等信息。

提示：如果被管服务器使用的是Linux/Unix家族操作系统，将不会显示调制解调器信息。

8.4.2.10 PCI附件

点击功能节点区的“服务器监视”-“资产信息”-“PCI附件”选项，即可进入PCI附件信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和IP信息，界面中显示了被管服务器的PCI附件设备名称和制造商等信息。

8.4.2.11 操作系统信息

点击功能节点区的“服务器监视”-“资产信息”-“操作系统”选项，即可进入操作系统信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和 IP 信息，界面中显示了被管服务器的操作系统类型、版本、补丁情况、已启动时间、注册用户、注册单位、注册产品 ID、安装日期等信息。

提示：对于Linux操作系统，没有专门的操作系统补丁栏目，补丁信息与操作系统版本信息放在一起。

8.4.2.12 IP 信息

点击功能节点区的“服务器监视”-“资产信息”-“IP 信息”选项，即可进入 IP 信息信息页面。

在主操作区上方显示有当前页面的管理位置以及服务器的名称和带内IP信息，界面中显示了被管服务器的 IP 地址信息，包括接口索引及对应的 IP 地址。下方显示的是被管服务器的接口信息，包括接口索引及对应的接口类型和带内MAC地址。

8.4.3 硬件健康信息

注意：硬件健康信息监控功能仅对具有 BMC 芯片的服务器有效。

8.4.3.1 温度

点击功能节点区的“服务器监视”-“硬件健康信息”-“温度”选项，即可进入服务器各个部件的温度监控信息页面。

用户可以看到现有的服务器温度传感器所得到的温度信息，包括传感器所在设备、读数、单位。同时，对于温度传感器，用户还可以进行阈值设置。

在阈置设计界面中将会有该阈值的报警上限、安全上限、安全下限（若有）、报警下限（若有）的设置滑块。这些限制值之间的大小关系是：

报警上限≥安全上限≥安全下限（若有）≥报警下限（若有）

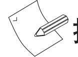
提示：系统不允许以上值的大小关系更改。例如若所设安全上限大于报警上

限，系统将会把所设的安全上限自动降至系统可接受的最大值，即等于报警上限的值。

8.4.3.2 电压

点击功能节点区的“服务器监视”-“硬件健康信息”-“电压”选项，即可进入服务器各个部件的电压监控信息页面。

用户可以看到现有的服务器电压传感器所得到的电压信息，包括传感器所在设备、读数、单位。同时系统默认设置了电压监控的阈值。

**提示：电压监控的阈值是不可以更改的！**

8.4.3.3 风扇

点击功能节点区的“服务器监视”-“硬件健康信息”- 风扇”选项，即可进入服务器各个部件的电压监控信息页面。

您将会看到现有的服务器风扇传感器所得到的风扇转速信息，包括传感器所在设备、读数、单位。同时系统默认设置了风扇转速监控的阈值。

**提示：风扇转速监控的阈值是不可以更改的！**

8.4.3.4 传感器

点击功能节点区的“服务器监视”-“硬件健康信息”-“传感器”选项，即可进入服务器各个部件的传感器信息页面。

用户可以看到现有服务器所有传感器的信息，包括传感器编号、类型、所在设备、读数、单位、阈值信息。

8.5 服务器控制

8.5.1 阈值设置

进入服务器监控页面，在左侧的功能节点区依次展开节点项目分类“服务器控制”就会看到服务器控制选项，点击功能节点区的“阈值设置”选项，即可进入服务器阈值设置页面。

您将会看到现有服务器所有的可设置阈值，并可以通过拖动滑块或直接输入值

对这些阈值进行设置。

在主机性能页面和温度页面，您还会在一些项目位置看到 图标，点击这个图标，也会弹出一个阈值设置的窗口，以供您对这一项目单独设置阈值。

在这里将会有各个阈值的报警上限、安全上限、安全下限（若有）、报警下限（若有）的设置滑块。这些限制值之间的大小关系是：

报警上限≥安全上限≥安全下限（若有）≥报警下限（若有）

提示：系统将不允许以上值的大小关系更改。例如若所设安全上限大于报警上限，系统将会把所设的安全上限自动降至系统可接受的最大值，即等于报警上限的值。

8.5.2 服务器控制

进入服务器监控页面，在左侧的功能节点区依次展开节点项目分类“服务器控制”就会看到服务器控制选项，点击功能节点区的“服务器控制”选项，即可进入服务器控制页面。

用户可以看到当前服务器的一些基本信息，包括：

- 服务器系统状态：表示当前服务器的电源状态；
- 前面板状态：显示当前服务器的前面板状态，该选项仅仅针对联想万全服务器有效；
- ID灯状态：显示当前服务器的ID开关状态，该选项仅仅针对联想万全服务器有效。

用户可以进行以下控制操作：

- 服务器操作系统控制：在服务器操作系统运行的状态下，允许用户关闭操作系统或者重启操作系统。
- 服务器电源管理：在服务器关机（电源关闭）的状态下，允许用户启动服务器；在服务器开机（电源开启）的状态下，允许用户关闭或者重启服务器。
- 服务器远程控制：针对联想万全服务器，用户可以锁定和解锁服务器的前面板。如果锁定服务器前面板，用户将无法使用服务器前面板的重启和开机按钮。用户还可以打开和关闭服务器前面板的ID灯、清除BMC的事件信息（清除SEL）。

- WOL 开机：对于一些服务器，在用户配置好的前提下，可以通过网络唤醒功能进行同一个网段内的开机。进行 WOL 开机，需要知道被控制服务器的 MAC 地址，还必须对服务器进行适当的配置，包括配置 BIOS 和配置网卡。通常是在服务器的 BIOS 的高级电源管理 APM 配置项中进行设置。

注意：服务器电源管理、服务器远程控制仅对安全了 BMC 芯片的服务器有效。而服务器前面板控制和服务器 ID 灯控制仅针对具有相应硬件配置的联想万全服务器有效！

注意：服务器在开机和关机的时候，会出现带外管理暂时中断的情况，这是因为在开机和关机的时候BMC绑定的网卡会断电并重新加电，此过程会导致管理通信中断。

提示：用户在清除 SEL 信息后，会收到一条服务器事件，描述为“传感器 16 发生事件”。这说明编号为16的传感器监测到SEL信息被成功清除了。

注意：用户在使用WOL的时候，唤醒服务器时候选择或者输入的服务器MAC地址，是带内管理的网卡MAC地址，不能使用带外管理的网卡MAC地址。带内管理的网卡 MAC 地址可以通过服务器资产信息的 IP 信息查看，带外管理的网卡 MAC 地址可以通过服务器资产信息的 BMC 芯片信息查看。

8.6 事件管理

服务器事件管理主要接收被管理服务器的各种产生事件。通过事件管理可以判断服务器是否发生问题，以及问题的严重程度。

对于接收到的事件，可以根据配置的告警策略进行事件的消息通知。同时用户可以对事件记录进行导出。提供 .xls 或 .csv 的导出文件格式。

进入服务器监控页面，在左侧的功能节点区依次展开节点项目分类“事件管理”，即可进入单服务器的事件管理页面。

关于事件管理的详细内容，请参见 9 *事件管理*。

8.7 告警策略配置

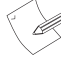
管理员可以设置告警的类型和告警的方式，统称为告警策略。系统提供4种告警方式：短信、电子邮件、SNMP Trap、浏览器界面告警。

- 短信：通过内置在管理中心上的短信硬件模块发送短信息；
- 电子邮件：通过管理中心可以连接的SMTP服务器发送电子邮件；
- SNMP Trap：管理中心向指定的IP地址列表发送SNMP Trap形式的告警；
- 浏览器界面告警：用户浏览器界面定时刷新获得当前事件所表示的服务器运行状态；

其中，浏览器界面告警不必进行策略设置，系统会自动针对阈值事件以此方式进行告警通知。其余3种告警方式都需要进行配置才能进行正常的告警通知，此模块的功能就是对这些告警策略进行配置。

此部分配置的告警策略为系统缺省使用的告警策略，即当服务器被加入到被管理服务器中后，在没有做其他设置时就会根据这里配置的告警策略进行各种方式的告警。同时，对于不同的被管理服务器还可以配置针对的告警策略。一般对某台服务器设置了单独的告警策略后，系统将会根据这台服务器配置的单机告警策略来进行告警。系统可以在某一时刻清除所有单服务器已经配置的告警策略，而强制所有服务器使用缺省的告警策略来进行告警通知。

服务器的告警策略配置的具体设置请参见11.5 *告警策略配置*。



提示：当全局服务器的告警策略配置和单机的告警策略配置同时存在时，会优先使用单机的告警策略配置进行事件消息的发送。

第九章 服务器事件管理

9.1 功能简介

服务器事件管理主要接收被管理服务器的各种产生事件。通过事件管理可以判断服务器是否发生问题，以及问题的严重程度。

对于接收到的事件，可以根据配置的告警策略进行事件的告警通知。同时用户可以对事件记录进行导出。提供 .xls 或 .csv 的导出文件格式。

9.2 界面概述

当管理中心接收到新事件，会在界面的左下角有图标闪动，以提示用户有新的事件发生。如下图所示：

发生新事件：

当用户点击该图标时会进入全局的事件管理页面，如下图所示：



您的位置：事件管理

导出Excel格式　导出CSV格式

□ 只显示未恢复的事件

□ 时间过滤

	服务器名称 全部	事件类型 全部	部件 全部	事件等级 全部	事件接收时间	描述	确认人 全部	明细
□	soc	性能事件	CPU	普通事件	2006-06-24 14:55:56	当前CPU利用率为33%,恢复正常	? 确认	
□	soc	性能事件	CPU	警告事件	2006-06-24 14:55:51	当前CPU利用率为86%,高于设定为80%的安全上限,仍然低于告警上限	? 确认	
□	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:46:36	盘符为I的IDE硬盘插入服务器	? 确认	
□	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:27:41	盘符为G的逻辑分区被创建	? 确认	
□	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:27:41	盘符为G的逻辑分区被删除	? 确认	
□	soc	安全事件	即插即用设备	警告事件	2006-06-24 14:26:01	盘符为G的未知磁盘设备插入服务器	? 确认	
□	soc	性能事件	CPU	普通事件	2006-06-23 20:47:28	当前CPU利用率为15%,恢复正常	? 确认	
□	soc	性能事件	CPU	严重事件	2006-06-23 20:47:18	当前CPU利用率为100%,高于设定为90%的告警上限	? 确认	
□	soc	性能事件	CPU	普通事件	2006-06-23 20:46:57	当前CPU利用率为6%,恢复正常	? 确认	

在全局事件管理列表中会显示事件的主要信息。包括服务器名称，事件类型，部件，事件等级，事件接收时间，描述，确认人，明细几部分。

提示：如果服务器存在同名，那么用户可以将鼠标移动到服务器名称之上，页面会自动弹出一个提示窗口，显示当前服务器的带内管理IP和带外管理IP。以此可以区别同名的服务器。

其中事件等级具有四级，严重性有低到高依次为普通事件，警告事件，严重事件，致命事件四个级别。

- 普通事件的显示图标为
- 警告事件的显示图标为
- 严重事件的显示图标为
- 致命事件的显示图标为

如果用户在服务器组织管理的服务器列表页面，会在出现问题的服务器左侧看到表示事件严重等级的图标，为用户提供了对应服务器的可恢复事件的浏览器页面告警。用户点击图标，就可以进入该服务器的事件管理页面。

9.3 基本操作

在事件列表页面，点击事件所在行的 图标，可以查看该条事件的明细信息。如下图示：

服务器名称	10.50.11.90
带内管理IP	
带外管理IP	10.50.11.90
部件	温度
来源	BMC硬件
事件类型	硬件健康事件
事件等级	警告事件
事件发生时间(服务器时间)	2006-05-26 00:00:50
事件接收时间(管理中心时间)	2006-05-25 16:09:35
描述	传感器48发生事件,温度高于安全上限
确认人	admin
确认时间	2006-05-25 18:48:06

增加了“带内管理 IP”，“带外管理 IP”，“来源”，“事件发生时间”，“确认时间”几项详细信息。

其中的“来源”一项显示事件的获取源。如果为“操作系统”代表事件是由慧眼的管理代理采集发送的。如果为“BMC 硬件”代表事件是直接通过带外管理的方式向被管服务器上的 BMC 芯片上获得的。

其中的“事件发生时间”代表被管服务器上产生事件的时间。

其中的“事件接收时间”代表管理中心接收到事件的时间。



提示：管理中心的时间可能与被管服务器的时间设定可能不同。故两个时间不具有横向的可比性。

在页面最下方显示了分页显示的状态，包括当前页码、总页数、总记录数、分页显示的每页显示条数。另外还包括分页操作按钮。其中：

- 点击显示第一页记录
- 点击显示上一页记录
- 点击显示下一页记录

- 点击显示最后一页记录

在 转到第 1 页 GO 可以直接输入想要查看的页码，点击GO后即可直接跳转倒该页。输入页码时应输入在总页数范围内的数字，如果输入的数字大于总页数则会跳转到最后一页。

9.4 事件过滤

在全局事件过滤可以根据服务器名称、事件的类型、发生事件的部件、事件的等级、是否恢复事件、确认人和事件发生的时间 7 个条件进行单一或组合过滤。

点击事件类型表头中的下拉选择框即可进行过滤现有的事件类型。其中，性能事件会包括 CPU 利用率事件，内存利用率事件，磁盘利用率事件。硬件健康事件包括各种从远程服务器上BMC控制芯片得到的事件。安全事件包括USB端口的插拔设备引发的事件。

点击事件等级表头的中的下拉选择框即可进行过滤所使用的事件的严重级别。严重性有低到高依次为普通事件，警告事件，严重事件，致命事件四个级别。

点击部件表头的中的下拉选择框即可进行过滤发生事件的部件。部件包括：内存、磁盘、CPU、温度、电压、风扇、其他。

点击确认人表头的中的下拉选择框即可进行过滤事件的确认者。在下拉选择框中显示了当前系统中存在的所有用户名和一个全部选项，一个其他人选项，一个尚未确认选项。其中，“全部”代表对确认人不作过滤，而“其他人”代表所有已被删除的用户和登录时使用的不存在的用户名。“尚未确认”条件可以将所有确认人为空的事件选择出来。

点击“只显示未恢复的事件”前的复选框会将只显示尚未恢复的事件。

点击“时间过滤”前的复选框则会出现时间过滤条件选择区。只有当勾选了时间过滤前的复选框并填写了时间范围才会使用时间过滤条件。在时间过滤范围的起始或终止框内任意位置点击鼠标即会显示时间选择面板，在时间选择面板上选择希望的时间后，在希望选择的天的方框内单击鼠标即可。当完成时间范围填写后点击时间过滤按钮即可使用填写的时间范围过滤日志记录。

如果只填写起始时间，则将过滤出填写时间之后发生的所有日志记录；如果只

填写终止时间，则将过滤出填写时间之前发生的所有日志记录。

时间过滤的条件是按照事件接收的时间来计算的，即管理中心的时间。

如果在全局的事件管理页面还可以对服务器名称进行过滤。

9.5 事件确认

当服务器出现问题时会产生事件,为了保证管理员可以对事件消息进行责任分配，系统提供了事件确认功能。当用户确认事件后，即表示该用户已经获得相应服务器发生问题的消息。系统会记录确认人和确认时间。

为了方便用户对多个事件进行确认。系统提供了批量确认功能。点击事件列表左下端的全选选择框，点击右侧的确认选定的事件连接即可将多个事件确认。

当事件已被确认过，则当全选时，该条事件会变灰，不可选择。

9.6 事件导出

用户可以将查询到的事件列表进行导出操作。可以导出为后缀为 xls 的 Excel 格式，或者是后缀为 csv 的逗号分割的文本格式。当点击事件列表页面中的导出 Excel 格式链接时，会弹出事件导出对话框。用户点击下载链接即可保存事件。

提示：为了保证导出效率，每个导出文件限制在1万条事件记录，如果事件记录大于 1 万条，提供多个文件下载。

如果您的机器上安装有 Excel 软件，并且选择打开一项，浏览器会自动调用 Excel，打开当前文档。如果选择保存一项，将导出的文件存在指定位置下。

提示：后缀为 csv 的文件可以直接使用文本编辑器进行查看。

9.7 事件告警

如果用户正确的配置的系统的告警设备参数，制定了有效的告警策略，就可以接收告警信息了。

事件可以通过邮件、短信、SNMP Trap 和浏览器页面四种方式进行告警。

邮件、短信、SNMP Trap需要事先定制好告警策略，否则将无法产生和接收告警事件。具体的配置方式参见 11.5 *告警策略配置*。

特别的，对于邮件和短信告警，用户还需要事先配置好发送邮件的参数，以及短信设备的通信参数。具体的配置方式参见系统配置管理的13.6*系统邮箱参数配置*和13.7*GSM Modem 参数配置*。

9.7.1 浏览器页面告警

浏览器页面告警不需要进行告警策略配置，只要系统接收到了事件，就会自动在页面底下的状态栏事件告警处弹出一个闪烁的图标。当用户点击该图标时会进入全局的事件管理页面，显示最新的事件。

同时，如果系统接收到的事件是可恢复事件，那么会在服务器组织管理的服务器列表页面中服务器左侧显示一个事件严重等级图标。用户点击该图标，可以进入该服务器的事件管理页面，查看导致产生该告警的未恢复事件。

提示：可恢复事件一类特殊的服务器事件。这类事件存在一定的逻辑关联，通常是一个事件表示服务器发生了告警，而另一个事件表示服务器的告警解除。

如果一台服务器接收到了某个事件的恢复事件，会自动将显示在服务器左侧的告警图标清除，表示告警已经解除。

用户也可以手工清除服务器的告警提示。用户首先选中需要清除告警提示的服务器，然后点击“重置状态”，就可以清除选中的服务器的告警提示了。

第十章 日志管理

10.1 功能简介

日志信息主要记录了使用本软件的若干重要操作的记录，如对设备的控制操作信息、开机关机信息、用户登录系统的记录信息等。

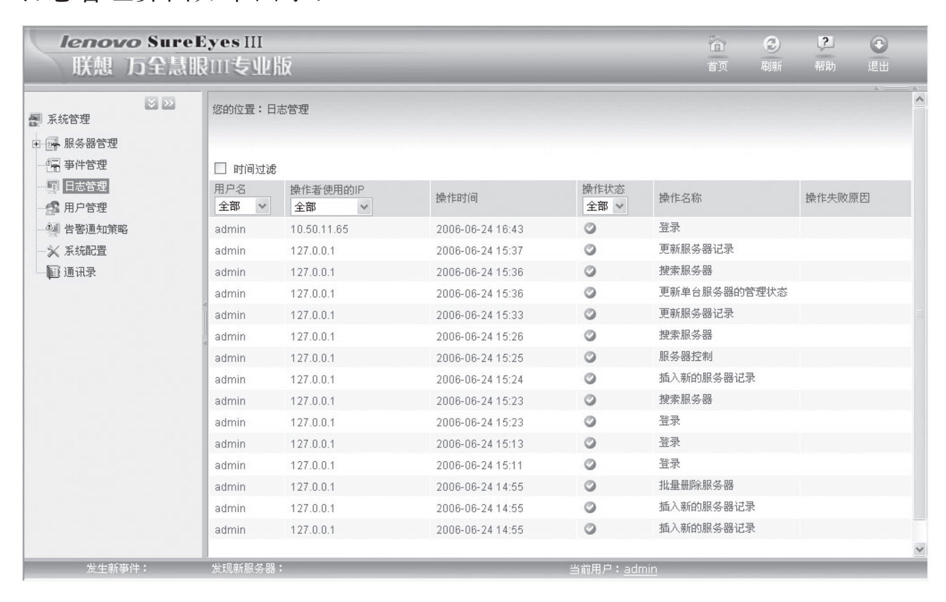
管理员可以对软件系统自动记录存储的日志信息进行的浏览、过滤等操作。

每条日志记录包括用户名、操作者使用的IP、操作时间、操作状态（成功或失败）、操作名称、操作失败原因（如果有）信息。

日志按照操作时间倒序排列显示，用户可根据需要按照用户名、操作者使用的IP、操作状态或操作时间过滤显示的事件记录。

10.2 界面概述

日志管理界面如下图示：



如图示，在界面中央区域显示的是当前系统记录的日志记录。日志记录分页显示，缺省显示第一页记录，即距离当前时间最近的日志。用户可以操作显示第一页、

上一页、下一页、最后一页或直接跳转至任意页。

在日志记录列表上方的时间过滤及复选框用于进行时间过滤，用户名、操作者使用的 IP 及操作状态表头中的下拉选择项用户进行用户名、IP 地址过滤和操作状态。

日志列表中的图标表示该条日志的操作状态为成功，图标表示该条日志的操作状态为失败。

10.3 基本操作

在页面最下方显示了分页显示的状态，包括当前页码、总页数、总记录数、分页显示的每页显示条数。另外还包括分页操作按钮：

点击显示第一页记录

点击显示上一页记录

点击显示下一页记录

点击显示最后一页记录

在 转到第 1 页 GO 可以直接输入想要查看的页码，点击 GO 后即可直接跳转倒该页。输入页码时应输入在总页数范围内的数字，如果输入的数字大于总页数则会跳转到最后一页。

10.4 日志过滤

日志浏览可以根据日志的用户名、日志的操作来源 IP 地址和日志发生的时间 3 个条件进行单一或组合过滤。

点击用户名表头中的下拉选择框即可选择进行过滤所使用的用户名。在下拉选择框中显示了当前系统中存在的所有用户名和一个其他人，其中其他人代表所有已被删除的用户和登录时使用的不存在的用户名。每次过滤时只能选择一个用户名进行过滤，选择后日志列表中将只显示出所选择的用户的所有日志记录。如果选择全部则代表不使用该过滤条件。

点击操作者使用的IP表头中的下拉选择框即可选择进行过滤所使用的IP地址。在下拉选择框中显示了当前系统记录的所有日志中出现过的 IP 地址。每次过滤时只能选择一个 IP 地址进行过滤，选择后日志列表将只显示出来自所选择的 IP 地址的日志记录。如果选择全部则代表不使用该过滤条件。

点击操作状态表头中的下拉选择框即可选择进行过滤所使用的操作状态。在下拉选择框中显示了成功和失败两种可能存在的操作状态。每次过滤时只能选择一种状态进行过滤，选择后日志列表将只显示出来自所选择的操作状态的日志记录。如果选择全部则代表不使用该过滤条件。

点击时间过滤前的复选框则会出现时间过滤条件选择区。只有当勾选了时间过滤前的复选框并填写了时间范围才会使用时间过滤条件。在时间过滤范围的起始或终止框内任意位置点击鼠标即会显示时间选择面板。在时间选择面板上选择希望的时间后，在希望选择的天的方框内单击鼠标即可。当完成时间范围填写后点击时间过滤按钮即可使用填写的时间范围过滤日志记录。如果只填写起始时间，则将过滤出填写时间之后发生的所有日志记录；如果只填写终止时间，则将过滤出填写时间之前发生的所有日志记录。

3种过滤条件可以任意组合使用，发生的过滤作用将互相叠加生成最后的日志显示结果。

第十一章 用户管理

11.1 功能简介

用户管理包括对用户的创建、修改、删除、修改权限等操作。

系统中的帐号分两种类型，一种是管理员帐号，还有一种是普通用户帐号。

• **管理员：**

管理员可以创建新的管理员帐号或普通用户帐号。所有的管理员帐号都具有管理系统所有的权限。

管理员帐号之间是互相可见的，当然也是可以互相修改和删除的。但是系统默认的 admin 帐号不能删除自身。

只有管理员帐号才可以创建和修改其它用户信息和权限配置。

• **普通用户：**

管理系统中的普通用户帐号只能由管理员帐号来创建。

普通用户只能监控管理员帐号分配的服务器，并且对服务器所能进行的操作也是有限的。

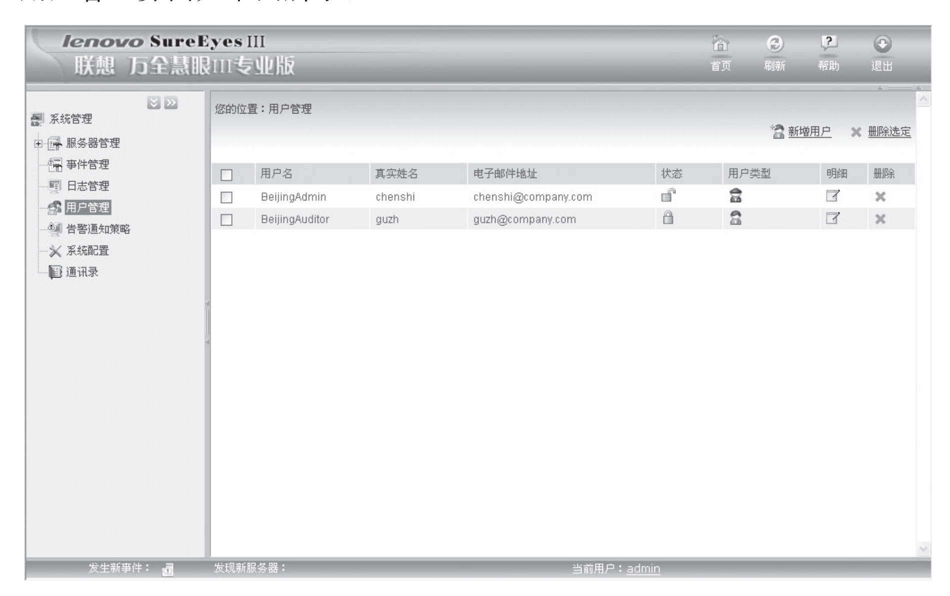
创建普通用户帐号时，要为其选择可以管理的设备范围，并且选择其拥有的操作权限。

SureEyes3 中可以有多名管理员和多名普通用户。

提示：admin 账号是系统默认账号，不能删除！

11.2 界面概述

用户管理界面如下图所示：



在用户管理中显示了系统当前创建的所有的帐号信息，可以通过对应的按钮或链接进行新增、修改、删除用户等的操作。

用户列表可以根据不同的需要按照不同的列进行正序或者反序排列显示。

如上图示，显示管理员和普通用户的显示情况。

图标🔒表示该帐号的状态为禁用，图标🔓表示该帐号的状态为启用；图标表示该帐号的类型为管理员，图标表示该帐号的类型为普通用户。

11.3 基本操作

1. 排序浏览

可以根据不同需要，按照不同的列对用户列表进行排序显示，排序的方式既可以正序也可以反序。如果需要进行排序显示，只需要点击希望排序的列的表头即可。在用户名后显示出▲图标，表示当前是按照用户名列正序排列的结果显示用户

列表。当此时再次单击用户名列的表头后，在用户名后显示出▼图标，表示当前时按照用户名列反序排列的结果显示用户列表。

其他列的排序操作亦如此。

2. 新增用户



点击用户管理界面的新增用户链接，即可弹出新增用户对话框。

在新增用户对话框中，显示有用户的所有属性，包括：用户登录名、真实姓名、密码、确认密码、固定电话、手机号码、电子邮件地址、序列号、状态、部门、描述和用户类型，其中标有 * 的属性为必填项。

提示：用户的类型一经选定将不能修改。

提示：用户名最长 15 个字符。

如果选择用户类型为普通用户，将显示出普通用户的权限分配区。普通用户的权限分别请详见 11.4 *用户权限分配*。

填写用户属性后，点击确定按钮即可完成新增用户操作。

新增用户时，使用的用户登录名必须是唯一的，不能与当前已经存在的任何帐号的登录名相同，否则将会显示报错界面，点击报错界面上的返回链接后，必须重复新增用户步骤，并选择新的有效用户名即可。

3. 修改用户属性

点击用户所在行的图标，即会弹出修改用户信息对话框。

修改用户信息对话框的操作与新增用户操作基本一致，最后点击确定按钮即可完成修改用户信息操作。

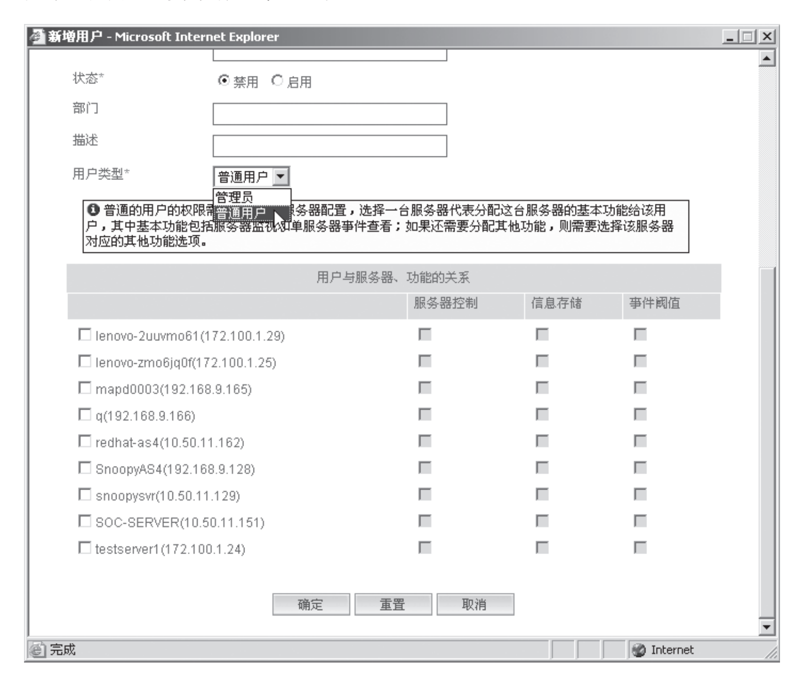
4. 删除用户

点击用户所在行的图标，即会弹出删除用户确认对话框，点击确定按钮即可删除该用户，点击取消按钮则放弃删除操作。

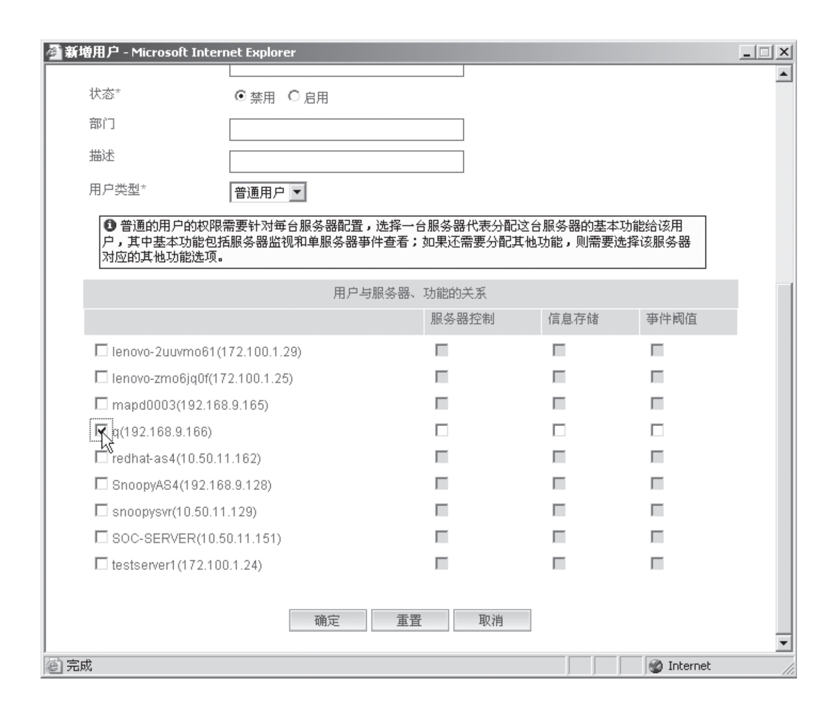
还可以通过选择用户所在行最左边的复选框,并点击 ✖删除选定 链接删除多个用户，同样会弹出确认对话框要求确认删除操作。

11.4 用户权限分配

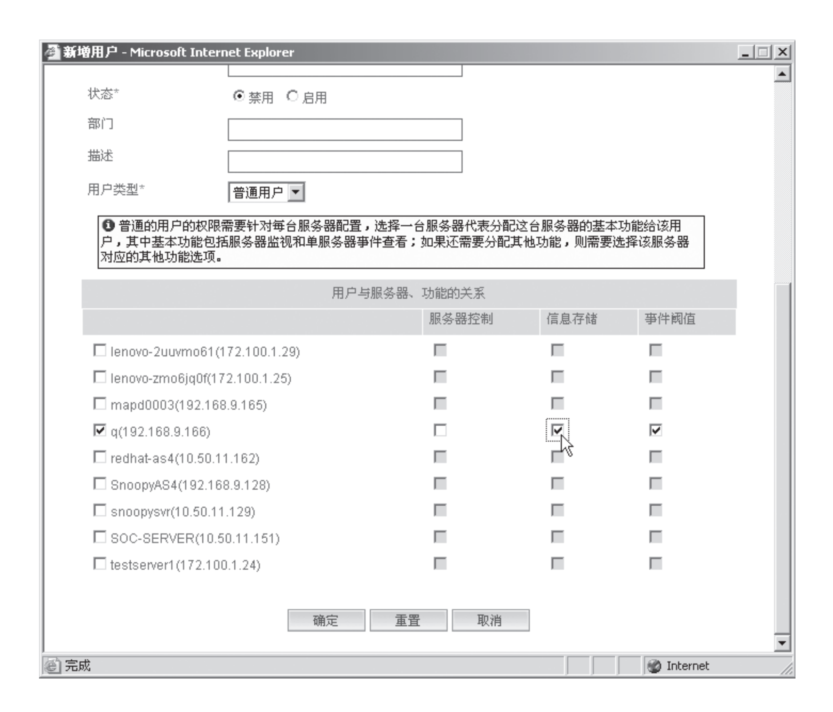
管理员具有系统的所有操作权限,但是普通用户的操作权限需要管理员在创建时进行分配。权限分配界面如下图示：



如图示，权限的分配分为两个纬度，一是可以管理的服务器，二是可以对被管理服务器的进行的操作。缺省条件下，普通用户不具有对任何服务器的任何操作权限，即如上图示。通过勾选服务器前的复选框可以制定用户可以管理的服务器，一旦选择了一台服务器，即代表对这台服务器享有了基本操作的权限，其中基本权限包括服务器的监视和服务器的事件查看功能。



如图示，即表明该用户可以对服务器 "q" 进行监视，并可以查看服务器 "q" 的事件。如果还希望该用户具有更多的功能，则可以根据需要继续选择其他功能。



如图示，即表示该用户不仅可以监视服务器“q”和查看服务器“q”的事件，同时还可以设置服务器“q”的监视项目的阈值，并可以设置服务器“q”的信息存储状态。

用户权限的分配还可以在修改普通用户信息的时候进行，操作与新增用户时相同。

11.5 权限控制

SureEyes3管理中心实现了基于用户管理的权限控制，只有属于用户管理列表中的用户才能登录和访问管理中心。不同的用户登录后能够使用的功能、管理的服务器都不尽相同，取决于该用户的权限。

普通用户登录后，除了只能对其有权控制的服务器进行基本管理（服务器监视、事件管理）之外，无法进行日志管理、用户管理、设置告警通知策略、进行系统配置，以及维护通讯录。普通用户也无法修改服务器的信息，彻底从管理列表中删除服务器。如果用户试图尝试没有授权的操作，将得到错误提示信息。

第十二章 告警策略配置

12.1 功能简介

通过配置告警策略系统可以将发生的事件以不同方式通知管理员，从而帮助管理员及时准确掌握服务器当前状态。

系统目前提供4种告警方式：短信、电子邮件、SNMP Trap、浏览器界面告警。

- 短信：通过安装在管理中心上GSM Modem发送短信息；（**GSM Modem为选配硬件设备，用户可以根据需要选购**）
- 电子邮件：通过邮件服务器以SMTP发送电子邮件；
- SNMP Trap：向指定的IP地址列表发送SNMP Trap形式的消息；
- 浏览器界面告警：浏览器界面定时刷新获得当前服务器的事件消息；

其中，浏览器界面告警不必进行策略设置。其余三种告警方式都需要进行配置。



提示：关于浏览器界面告警的说明，详见事件管理中的9.7 *事件告警部分*。

告警策略的配置分为全局配置和单服务器配置两部分。当全局服务器的告警策略配置和单机的告警策略配置同时存在时，会优先使用单机的告警策略配置进行事件消息的发送。

12.2 界面概述

告警策略配置的界面如下图所示：

显示导航

您的位置：告警通知策略

覆盖所有单服务器设置 ☐ 注意：您选择此项将覆盖以前所有对单服务器的设置，请谨慎！

☑ 发送短信警报*

直接添加接收人手机号码 [ ] 添加

接收人手机号码

短信接收列表

<<

常用联系人

删除选定

事件等级

普通事件
警告事件
严重事件
致命事件

☑ 电子邮件警报*

直接添加接收人邮件地址 [ ] 添加

接收人邮件地址

邮件接收列表

<<

常用联系人

删除选定

事件等级

普通事件
警告事件
严重事件
致命事件

☑ 发送SNMP Trap警报*

添加接收IP地址 [ ] 添加

接收IP

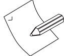
删除选定

事件等级

普通事件
警告事件
严重事件
致命事件

应用 重置

如果需要配置某一种告警方式，则可以点击告警方式前的复选框。



提示：如果选择了覆盖所有单服务器的设置，即界面中有红色字体提示的选择框。系统将会清除所有单机告警策略。

12.3 发送短信警报

对于接收人手机号码，既可以通过从通讯录中直接选择，也可以手工输入任意号码。如果通过通讯录选择，则在常用联系人列表中选择要使用的联系人，点击 << 按钮或者直接在联系人名称上双击鼠标即可。

注意：在设置短信警报策略的时候，从通讯录的联系人中选择一个手机号码加入短信接收列表中，然后在通讯录中更改此联系人的手机号码，再回到短信警报策略页面，常用联系人的手机号码自动更新，但是先前添加到短信接收列表中的手机号码不会做相应改变。

如果手工输入，则在“直接添加接收人手机号码”后的输入框输入号码，并点击添加按钮即可。

如果想从短信接收列表中删除手机号码，则直接在短信接收列表中选择希望删除的手机号码后，点击下方的删除选择按钮即可。

事件的等级预定义为四种，分别是普通事件、警告事件、严重事件和致命事件。对于事件等级的选择可以选择一个也可以选择多个。选择多个事件等级时，既可以直接使用鼠标拖动选择，也可以通过使用 Ctrl 或 Shift 键配合鼠标选择（操作同时选择多个文件）。

用户接收到的短信为以 "/" 分割的关键字，格式如下：

服务器名 / 带内管理 IP/ 带外管理 IP/ 部件 + 事件等级 / 事件接收时间 (管理中心时间)

举例如下：

SERVER-A/192.168.0.1/10.50.11.50/CPU 警告事件 /2006-3-21 19:32:12

12.4 电子邮件警报

对于接收警报的邮件地址，既可以通过从通讯录中直接选择，也可以手工输入

任意邮件地址。如果通过通讯录选择，则在常用联系人列表中选择要使用的联系人，点击 << 按钮或者直接在联系人名称上双击鼠标即可。

注意：在设置电子邮件警报策略的时候，从通讯录的联系人中选择一个邮件地址加入到邮件接收列表中，然后在通讯录中更改此联系人的邮件地址，再回到电子邮件警报策略页面，常用联系人的邮件地址会自动更新，但是先前添加到邮件接收列表中的电子邮件地址不会做相应改变。

如果手工输入，则在“直接添加接收人邮件地址”后的输入框输入地址，并点击添加按钮即可。

如果想从邮件接收列表中删除邮件地址，则直接在邮件接收列表中选择希望删除的邮件地址后，点击下方的删除选择按钮即可。

事件的等级预定义为四种，分别是普通事件、警告事件、严重事件和致命事件。对于事件等级的选择可以选择一个也可以选择多个。选择多个事件等级时，既可以直接使用鼠标拖动选择，也可以通过使用 Ctrl 或 Shift 键配合鼠标选择（操作同时选择多个文件）。

用户接收到的邮件内容会包括：服务器名称、带内管理 IP、带外管理 IP、部件、来源、事件类型、事件等级、发生时间（服务器时间）、接收时间（管理中心时间）和描述。

举例：管理员收到的邮件的主体如下所示：

服务器名称：SERVER – A

带内管理 IP：10.50.11.112

带外管理 IP：

部件：内存

来源：操作系统

事件类型：性能事件

事件等级：警告事件

发生时间（服务器时间）：2006-05-11 17:36:19

接收时间（管理中心时间）：2006-05-11 17:36:20

描述：当前内存利用率为 85%，低于设定为 90% 的告警上限，仍然高于安全上限

12.5 发送 SNMP Trap 警报

接收警报的 IP 地址，可以在添加接收 IP 地址后的输入框直接输入，并点击添加按钮即可。

如果想从接收 IP 列表中删除地址，则直接在接收 IP 列表中选择希望删除的 IP 地址后，点击下方的删除选择按钮即可。

事件的等级预定义为四种，分别是普通事件、警告事件、严重事件和致命事件。对于事件等级的选择可以选择一个也可以选择多个。选择多个事件等级时，既可以直接使用鼠标拖动选择，也可以通过使用 Ctrl 或 Shift 键配合鼠标选择（操作同时选择多个文件）。

第十三 系统配置管理

13.1 功能简介

管理员可以通过此功能对软件系统进行系统日志管理、用户权限管理、系统参数配置等的管理。

系统配置对象包括：

• 日志保存策略；
• 事件记录保存策略；
• 系统缺省每页显示的记录数；
• 系统邮箱参数；
• GSM Modem 参数；
• 系统密码策略；
• 监控刷新频率；

13.2 界面概述

系统配置界面如下图所示：

显示导航
您的位置：系统配置

全部展开 全部收拢

日志保存策略配置*
保留时间 1月

事件记录保存策略配置*
保留时间 30日 是否生效
保留大小 5000条 是否生效

系统缺省每页显示的记录数*
15

系统邮箱参数配置
发件人姓名
发件人邮件地址
发送邮件服务器(SMTP)地址
发送邮件服务器需要身份验证
测试邮箱

GSM Modem参数配置
连接端口 COM1
通讯速率 9600
厂商 未发现
型号 未发现
测试连接

用户密码策略（下次登录后生效）*
密码最小长度* 6
密码是否需要数字字母混用* 是
密码是否允许与用户名相同* 否
密码最小修改时间(天)* 30 (0表示不限制)

监控刷新频率配置*
高速* 30 秒刷新一次
中速* 60 秒刷新一次
低速* 300 秒刷新一次

应用 重置

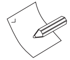
如上图，所有的配置项目均处于收缩状态。点击配置项目图标和名称前的 即可展开配置项目进行设置，再次点击配置项目图标和名称前的 即可再次收缩配置项目。

13.3 日志保存策略配置

日志保存策略的配置是针对系统的日志管理中的所有日志记录的保存事件进行的。

系统中所有的操作日志记录按照时间先后分月存储，系统可以根据用户的配置，选择保存最近一个月、两个月或三个月的日志记录。如上图，用户只需从下拉选项中选择一个时间长度即可。如果选择保存最近一个月的日志记录，则系统将自动保存当月的日志记录，并删除上月的所有日志记录。

日志的缺省保存时间为1个月。



提示：出于系统性能和日志查找的效率考虑，由于日志记录量较大，建议不要设置保存太长时间。

13.4 事件记录保存策略配置

事件记录保存策略的设置是针对所有服务器产生的事件记录在管理中心的存储事件和清除条件进行的。

用户可以选择只保留选定事件长度的事件记录或只保留选定数量的事件记录或者两者同时使用。在同时选择的情况下，如果哪个条件先符合要求，则会相应地执行其事件整理操作。

要使设置的保存策略生效，必须在策略后对应的是否生效复选框中进行选择。

缺省地，系统对事件保留时间30天，同时保留数量为5000条。

13.5 系统缺省每页显示的记录数

此配置是针对系统如日志管理等存在分页列表显示页面中每页显示的记录数量进行的。

可以选择的每页显示的记录数量为：15条、20条、25条、30条。

缺省为每页显示15条记录。

13.6 系统邮箱参数配置

系统邮箱参数配置是针对当系统需要向外发送电子邮件时（如发送电子邮件事件警报）所使用的邮箱地址等参数进行的。

系统邮箱的参数包括：发件人姓名、发件人邮件地址、发送邮件服务器(SMTP)地址和发送邮件所需要的身份验证信息用户名及密码。

注意：SureEyes3 不支持中文电子邮箱。

如果发送邮件服务器需要在发送邮件时验证身份，则需要同时配置发送时使用的帐号和密码。点击发送邮件服务器需要身份验证前的复选框，即可展开输入帐号和密码部分。

在填写了邮箱设置后可以测试刚刚设置的邮箱是否可以正常使用。点击测试邮箱按钮，按钮文字即变为“测试中 ...”，且按钮不再可以点击。如果邮箱可以正常使用则弹出成功通知对话框，如果邮箱无法正常使用则同样弹出失败通知对话框。

如果发送邮件服务器地址填写了无效的地址格式，则在提交修改结果时，界面将提示错误。

13.7 GSM Modem 参数配置

如果用户需要使用短信进行告警配置，首先需要对GSM Modem进行配置检测。

根据用户选购的GSM Modem不同，配置步骤不同。以典型的PCI接口的GSM Modem 为例说明，配置检测步骤如下：

第一步：PCI 接口 GSM MODEM 与计算机主板的连接

将PCI接口GSM MODEM直接插入计算机主板的空PCI插槽中，用螺丝固定，并使用配套的数据线连接 Modem 到服务器的串口上。

第二步：安装 SIM 卡

将 SIM 卡插入 GSM MODEM 侧面的 SIM 读卡器中，SIM 卡有芯片的一面与读卡器紧密接触，并锁紧。



提示：插入 SIM 卡之前，请确认 SIM 卡能够正常地发送和接收短信息。

第三步：检测工作状态

完成以上操作，打开电源，红色 ID 亮，待红灯闪亮时，即表示 GSM MODEM 进入正常工作状态。

第四步：管理中心检测

根据实际连接的端口选择对应的“连接端口”和“通讯速率”，并点击“测试连接”按钮。如果Modem可以被正常被检测到，会显示检测到的“厂商”，“型号”。如果 Modem 不能被正常检测，请更改配置，再次进行连接测试。

13.8 系统密码策略

系统密码策略的设置是针对用户管理中帐号所使用的密码所需要符合的一定的要求进行。

密码策略包括对密码最小长度的限制、是否强制密码必须使用数字与字母混合的方式、是否不允许使用与用户名相同的密码和密码的最长使用时间。

密码的最小长度限制缺省为6个字符长度，用户可根据实际情况修改，但最小长度必须大于0。

密码最小修改时间缺省为30天，即从用户上次修改密码时算起（如果为新建用户则从创建时间起）30天后系统会提示用户修改密码。用户可根据实际情况修改，如果改为0则表示密码没有最长使用时间的限制，即系统始终不会提示用户修改使用时间过场的密码。

缺省地，密码强制使用数据与字母混合方式，并且不允许密码和用户名相同。

如果密码最小长度或密码最小修改时间填写了无效的数值，则在提交修改结果时，界面将提示错误。

13.9 监控刷新频率配置

监控刷新频率配置是针对服务器监视时不同的监视项目的页面自动刷新时间进行的。

服务器监视时，根据不同的监视项目会具有不同的刷新频率。刷新的频率分为三个级别：快速、中速和慢速。如平均CPU的利用率为高速刷新，逻辑CPU的编号为低速刷新，等等。针对不同级别的刷新频率用户可以根据实际的需要自行配置，缺省情况下高、中、低三速的刷新间隔分别为30、60、300秒。

如果刷新频率填写了无效的数值，则在提交修改结果时，界面将提示错误。

第十四章 通讯录

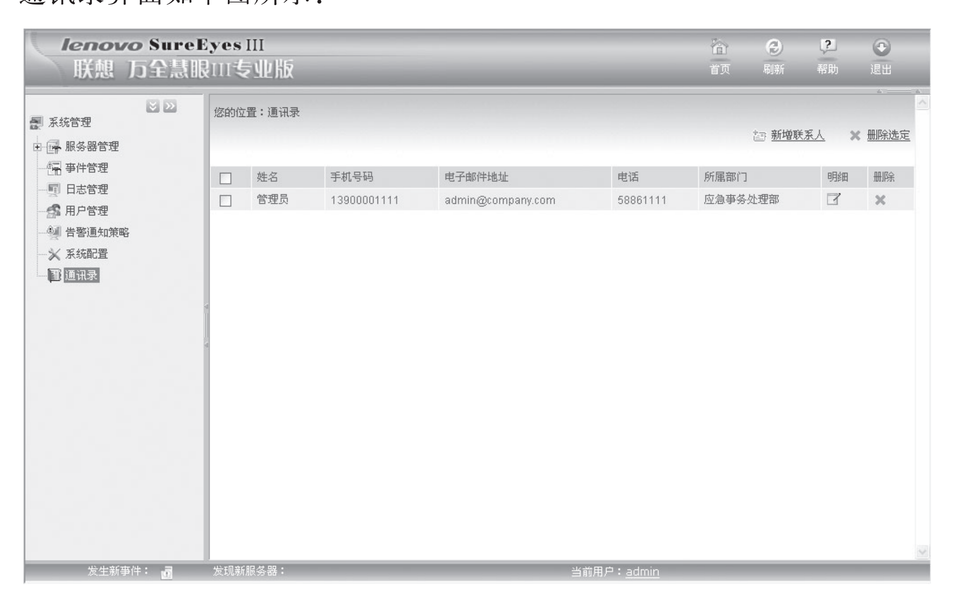
14.1 功能简介

通讯录的主要功能是提供用户一个联系人列表,以便于在配置告警策略时可以方便的通过选择联系人的方式直接填写接收短信或邮件告警人的手机号码或电子邮件地址。

联系人的信息包括：姓名、手机号码、电子邮件地址、电话、所属部门和其他信息。

14.2 界面概述

通讯录界面如下图所示：



在通讯录界面列表显示了当前系统中存在的所有通讯录记录。

通讯录列表可以根据不同的需要按照不同的列进行正序或者反序排列显示。

在通讯录界面可以方便的对联系人进行新增、修改、删除操作。

14.3 基本操作

1. 排序浏览

可以根据不同需要，按照不同的列对联系人列表进行排序显示，排序的方式既可以正序也可以反序。

如果需要进行排序显示，只需要点击希望排序的列的表头即可在姓名后显示出图标，表示当前是按照姓名列正序排列的结果显示联系人列表。当此时再次单击姓名列的表头后，在姓名后显示出图标，表示当前时按照姓名列反序排列的结果显示联系人列表。其他列的排序操作亦如此。

2. 新增联系人

点击通讯录界面的新增联系人链接，即会弹出新增联系人对话框。

新增联系人时需要填写的联系人信息包括：姓名、手机号码、电子邮件地址、电话、所属部门和其他信息。其中标注有*的信息为必填信息，即姓名、手机号码和电子邮件地址。填写信息时，直接在各个信息后对应的输入框内输入即可。填写完毕后点击确定按钮即可完成新增联系人操作。

3. 修改联系人信息

在通讯录界面点击希望修改的联系人所在行的图标，即会弹出修改联系人信息对话框。

修改联系人信息时操作于新增联系人的操作是一致的，完成后点击确定按钮即可完成修改操作。修改后即可在通讯录界面实现出修改后的结果。

4. 删除联系人

删除联系人时可以在通讯录界面点击希望删除的联系人所在行的图标即可，点击后即会弹出删除确认窗口。

点击确定按钮即可完成删除操作，点击取消按钮则会放弃删除操作。

删除联系人还可以通过在希望删除的联系人所在行最前方的复选框内点击选中，再点击通讯录界面的删除选定链接的方式实现。点击链接后，同样会弹出删除确认窗口。通过这种方式，可以同时删除多个联系人记录。

另外可以通过点击表头所在列最左侧的复选框来全部选择所有联系人和取消对所有联系人的选择。

第十五章 服务器远程控制工具

15.1 功能简介

注意：使用该控制工具之前，请确认待控制的服务器具有 BMC 芯片！

服务器远程控制工具的功能包括 IDER（IDE 设备重定向）和 SOL（基于网络的串口重定向）。

IDE设备重定向主要是将远程控制工具所在的主机的IDE设备通过网络重定向至服务器，使没有软驱或光驱的服务器可以从该主机的软驱或光驱引导系统。

串口重定向主要是将服务器的串口信息通过网络重定向至远程控制工具所在的主机，使用户可以远程操作服务器，包括查看服务器的 POST 过程、进行 RAID 和 BIOS 设置以及接管 DOS 系统操作。

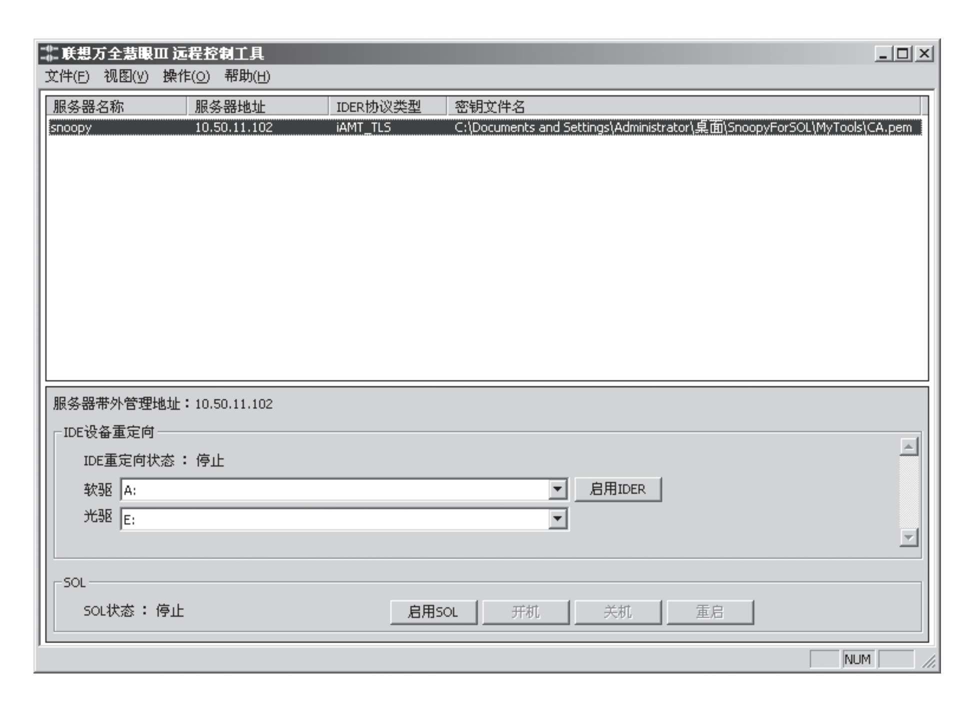
通过 SureEyes3的远程控制工具，管理员可以将本地 IDE 设备虚拟成远程服务器的 IDE 设备，并通过 IPMIv2.0 定义的 SOL（Serial over LAN）功能远程接管服务器的开机过程，使用户有机会进行远程的服务器诊断和修复。

服务器远程控制工具直接和服务器 BMC 芯片进行通信。

15.2 界面概述

运行远程控制工具后，会自动在操作系统的托盘区出现一个图标，同时打开程序主窗口。

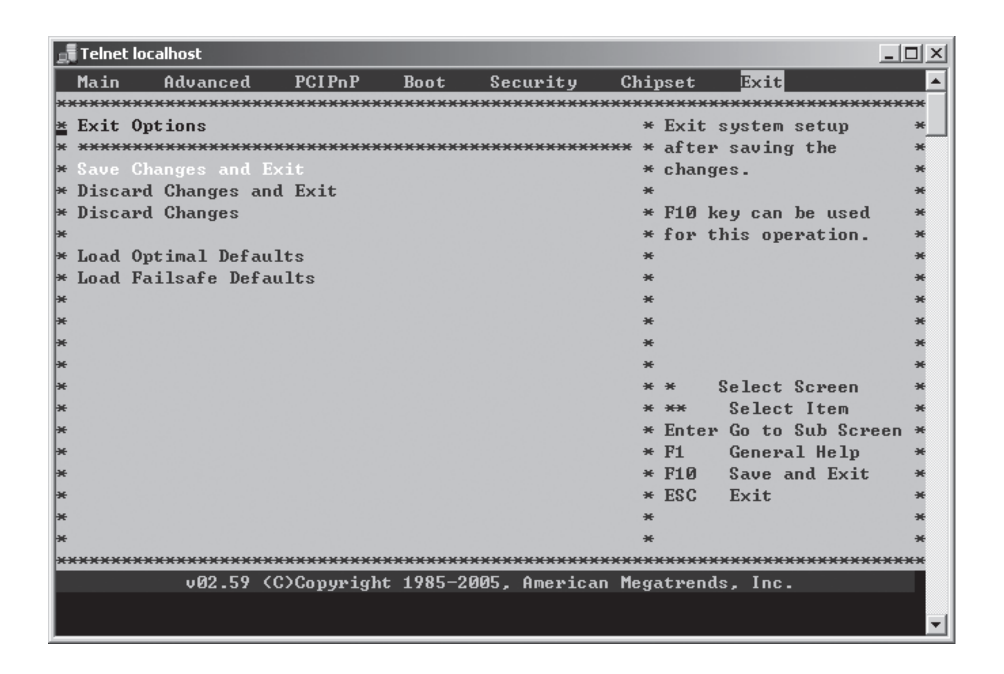
程序主界面如下：



界面的开始部分显示了已经添加的服务器列表，显示有服务器的名称、地址、重定向的通信协议和通信时使用的密钥文件。可以通过选择菜单“操作”→“添加服务器”来添加更多的服务器。

服务器列表以下是操作区：主要有两部分的操作区域，分别是IDE重定向操作（IDER）和串口重定向（SOL）操作。

启用 SOL 后出现的 SOL 控制台界面举例如下：



15.3 IDE 重定向

IDE 重定向也称为 IDER。使用 IDE 重定向功能需要事先配置好被管理服务器的 BIOS，并在被管理服务器上生成 IDE 重定向证书。然后，用户可以在安装了服务器远程控制工具的控制台使用 IDER 证书对服务器进行 IDE 重定向操作。

15.3.1 生成 IDE 重定向证书

在使用IDE重定向之前，需要首先在服务器端生成一个安全证书，用以对IDER 的通信过程进行加密，确保 IDER 的安全性。生成 IDER 证书的工作必须在被管理的那台服务器上进行，而且必须在 PC-DOS 环境下进行。

注意：用户要使用证书生成工具，必须在 PC-DOS 环境下！用户必须使用万全慧眼附带的安装光盘引导服务器，重新启动后，即可进入 PC-DOS 环境。在使用安装光盘重新引导服务器之前，请查看服务器BIOS设置，确认启动顺序，确保第一启动设备是光驱。

PC-DOS 启动的时候，会自动加载光驱驱动和 USB 设备驱动。在系统提示是否需要开始检测 USB 设备的时候，用户可以插入需要用于导出 IDER 证书的 USB 存储设备，并按下回车（Enter）键。系统会自动加载并启用 USB 存储设备。如下图所示：

```
Extended Memory Specification (XMS) Version 3.0
Copyright (C) IBM Corp. 1988, 1994

WARNING: Invalid parameter ignored: /TESTMEM:OFF
Installed A20 handler number 2.
64K High Memory Area is available.



This driver is provided by Oak Technology, Inc..
OTI-91X ATAPI CD-ROM device driver, Rev D91XV352
(C)Copyright Oak Technology Inc. 1987-1997
  Device Name         : MSCD000
  Transfer Mode       : Programmed I/O
  Number of drives    : 1


ASPI Manager for USB mass-storage  Version 2.20
 (C)Copyright Panasonic Communications Co., Ltd. 2000-2004

   ==============================================
   ===  Connect the target device to USB port. ===
   ===  Press [ENTER] to continue.             ===
   ==============================================
_
```

提示：如果被管理的服务器具有软驱，用户也可以选择使用软驱作为导出 IDER 证书的介质，而不必加载 USB 存储设备。但是，用户必须从软盘和 USB 存储设备中选择其中一种作为导出介质，一般无法使用服务器自带的硬盘设备，因为 PC-DOS 只能识别 FAT16 格式的硬盘文件系统。

PC-DOS 启动成功，会自动建立一个内存磁盘（RAMDRIVE），生成 IDER 证书所需的软件放在该内存磁盘下，并且系统会自动将当前驱动器号定位到该内存磁盘下。用户进入 ider 目录，使用 cergent.bat 命令即可运行证书生成工具。

运行 cergen.bat，命令格式为：cergen < server-name> <cert_file-name>，其

中 server_name 是该服务器的名称，建议使用该服务器的带外管理 IP 地址作为 server-name；cert_file-name 表示生成的证书文件名，建议以 der 为证书文件扩展名。成功执行后在当前目录下产生证书文件。用户可以使用 copy 命令将证书文件复制到软盘或者 USB 存储介质中，以备后用。

注意：用户在加载USB存储设备后，不能拔出USB接口，否则再插入后就无法识别了。

15.3.2 设置服务器 BIOS

在使用 IDER 之前，需要设置被管理服务器的 BIOS，启用 IDER 功能。

用户进入 BIOS 配置界面后，选择“Advanced”功能，选择“ESB2 BMC Configuration”，进入 IDER 配置界面，设定“BMC IDE-Redirection Support”为 Enabled，表示启用 IDER。

15.3.3 IDE 重定向

用户在配置好被管理服务器，生成了服务器 IDER 证书后，就可以开始使用 IDER 功能了。使用 IDER 的步骤如下：

1) 将在服务器上生成的证书拷贝到远程控制工具所在的主机上。
2) 从“开始”-“程序”-“万全慧眼 3”菜单运行“远程控制工具”。
3) 首先添加服务器，选择菜单“操作→添加服务器”，在弹出对话框中，输入服务器名称和带外管理 IP 地址；密钥文件选择先前生成的 ca.der 文件。确定添加即可。

注意：添加服务器的时候，输入的服务器名称必须和生成证书的时候服务器名称保持一致！输入的服务器 IP 地址，必须是带外管理 IP 地址，而不能使用带内管理 IP 地址！

4) 在服务器列表中选择要操作的服务器，然后在IDE设备重定向操作区域确定需要重定向的 IDE 设备，包括软驱和光驱，完成后点击“启用”按钮。
5) 成功执行后，此时在服务器端就能正常使用远程IDE设备了。否则将弹出错误对话框提示 TLS 通信失败，此时请检查密钥文件是否正确或服务器地址是否正确。

注意：用户在指定重定向设备的时候，必须同时指定光驱和软驱，否则重定向将失败！

提示：用户添加服务器成功，会在系统目录的 \System32\Drivers\etc\HOSTS 文件中添加一条记录，形如：
<server-ip> <server-name>
其中 server-name 对应添加服务器时填写的服务器名称。
如果用户在使用 cergen 命令生成证书的时候，使用服务器 IP 地址作为服务器名称，那么在远程控制控制工具中添加服务器的时候，就不会修改 HOSTS 文件。

IDER 运行的时候，用户可以在被管理服务器上看到虚拟的软驱或者光驱。用户可以使用这些软驱或者光驱，就象使用本地 IDE 设备一样。

15.4 串口重定向

串口重定向也称为SOL。使用串口重定向功能需要事先配置好被管理服务器的BIOS和BMC芯片。然后，用户可以在安装了服务器远程控制工具的控制台对服务器进行 SOL 重定向操作。

15.4.1 设置服务器 BIOS

在使用 SOL 之前，需要设置被管理服务器的 BIOS，启用 SOL 功能。

用户进入 BIOS 配置界面后，选择“Advanced”下的“Remote Access Configuration”，进入 SOL 配置界面，设定“Remote Access”为 Enabled，表示启用 SOL，同时设定“Serial port number”为 COM3，如下图所示：

```
            Advanced

Configure Remote Access type and parameters
****************************************************
Remote Access                          [Enabled]

Serial port number                     [COM3]
     Base Address, IRQ                 [AF00h, 7]
Serial Port Mode                       [19200 8,n,1]
Flow Control                           [None]
Redirection After BIOS POST            [Always]
Terminal Type                          [ANSI]
VT-UTF8 Combo Key Support              [Enabled]
Sredir Memory Display Delay            [No Delay]
```

15.4.2 配置 BMC 芯片

由于SOL功能是由内置在服务器上的BMC芯片提供的，因此，需要配置BMC芯片，启用 SOL 功能。配置 BMC 必须在 PC-DOS 环境下进行。

注意：用户要使用BMC配置工具，必须在PC-DOS环境下！用户必须使用万全慧眼附带的安装光盘引导服务器，重新启动后，即可进入 PC-DOS 环境。在使用安装光盘重新引导服务器之前，请查看服务器BIOS设置，确认启动顺序，确保第一启动设备是光驱。

用户进入 PC-DOS 后，使用 bmccfg 命令进行 SOL 配置。在 bmc 配置命令提示符下使用 get -t sol 1 可以获取网卡 1 的 SOL 配置信息，具体获取方法参见 16.1.2 *获取当前 SOL 配置*；使用 set -t sol 命令可以配置 BMC 的 SOL 信息。具体配置方法参见 16.2.3 *配置 SOL*。

15.4.3 SOL

用户在配置好被管理服务器的BIOS和BMC后，就可以开始使用SOL功能了。使用 SOL 的步骤如下：

1) 从“开始” − “程序” − “万全慧眼 3”菜单运行“远程控制工具”。
2) 在服务器列表中选择要操作的服务器，然后在 SOL 操作区域，点击“启用 SOL”按钮，打开 SOL 控制台窗口。
3) 如果此时被管理的服务器处于关机状态，那么用户可以通过点击“开机”按钮启动服务器，同时在SOL控制台窗口看到服务器POST过程。此时，用户可以在SOL控制台窗口中进行各种远程操作，包括BIOS设置，RAID配置、接管DOS操作界面，等等。如果此时被管理的服务器出于开机运行状态，那么用户可以通过点击“重启”按钮或者“关机”和“开机”按钮启动服务器，同时在 SOL 控制台窗口看到服务器 POST 过程。

第十六章 BMC 配置

注意：使用 BMC 配置工具之前，请确认待配置的服务器具有 BMC 芯片！

用户在使用带外管理方式进行服务器管理，以及使用 SOL 功能的时候，需要进行 BMC 配置。用户可以通过 BMC 配置工具随时修改服务器带外管理的参数。

BMC 配置工具运行在 PC-DOS 系统之下，包括两个程序，分别为 bmccfg.exe 和 cmdtool.exe，位于安装光盘的 bmc 目录。用户使用可启动的安装光盘可以使服务器进入 PC-DOS 环境。

注意：用户要使用BMC配置工具，必须在PC-DOS环境下！用户必须使用万全慧眼附带的安装光盘引导服务器，重新启动后，即可进入 PC-DOS 环境。在使用安装光盘重新引导服务器之前，请查看服务器BIOS设置，确认启动顺序，确保第一启动设备是光驱。

PC-DOS 启动成功，会自动建立一个内存磁盘（RAMDRIVE），进行 BMC 配置所需的软件放在该内存磁盘下，并且系统会自动将当前驱动器号定位到该内存磁盘下。用户进入 bmc 目录，运行 bmccfg.exe 即可运行 BMC 配置工具。

一般联想的服务器上会集成两块网卡。用户可以通过BMC配置工具对每一块网卡进行BMC设备设置和管理。BMC配置工具提供了三种BMC管理功能：配置 BMC 网络、配置 BMC 管理密码和 SOL（Serial Over LAN）配置管理。

- **配置网络**

用户可以在每一块网卡上，修改和管理 BMC 的网络配置。网络配置包括：带外 IP 地址、带外网关地址、带外子网掩码和带外网络类型。

- **配置 BMC 管理密码**

提供了修改 BMC 设备用户的访问密码功能。

- **SOL 配置管理**

BMC设备提供了SOL功能，用户可以通过SOL配置管理，选择哪一块网卡支持 SOL 功能，并且可以设置 SOL 功能的数据传输率（Baud Rate）。

在 BMC 配置程序的命令行状态下，用户可以使用以下内部命令：

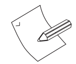
- Help [-C < command >] 显示内部命令说明列表或者显示某条命令的详细说明列表
- Exit/quit 退出的 bmccfg 工具
- Version 显示工具的版本号
- Clear 清除交互式界面
- Get -T <target> <options> 获得 BMC 配置信息
- Set -T <target> <options> 设置 BMC 配置信息

下表列出了所有内部命令。

内部命令	功能描述
Help	显示 BMC 配置工具所有的内部命令和内部命令的帮助信息
Help -c command	显示 BMC 配置工具指定的内部命令帮助信息
Exit	退出 BMC 配置工具
Quit	退出 BMC 配置工具
Version	显示 BMC 配置工具版本
Clear	清空 BMC 配置工具显示屏幕
Get -h	显示 Get 命令的帮助信息
Get -h network	显示 Get 命令中网络设置部分的帮助信息
Get -t network eth_id	显示编号为eth_id的网卡的网络设置信息，网络设置信息包括了网络类型、IP 地址
Get -t network eth_id ip	显示编号为 eth_id 的网卡的 IP 地址
Get -t network eth_id subnet	显示编号为 eth_id 的网卡的子网掩码
Get -t network eth_id gateway	显示编号为 eth_id 的网卡的网关地址
Get -t network eth_id type	显示编号为 eth_id 的网卡的网络类型
Get -h sol	显示 Get 命令中 SOL 设置部分的帮助信息
Get -t sol eth_id	显示编号为eth_id的网卡的SOL配置信息，包括SOL 功能是否有效、SOL 的波特率
Get -t sol eth_id config	显示编号为 eth_id 的网卡的 SOL 是否启用
Get -t sol eth_id baud	显示编号为 eth_id 的网卡的 SOL 通信波特率
Set -h	显示 Set 命令的帮助信息
Set -h network	显示 Set 命令中网络设置部分的帮助信息

Set -t network eth_id ip <value>	设置编号为 eth_id 的网卡的 IP 地址
Set -t network eth_id subnet <value>	设置编号为 eth_id 的网卡的子网掩码
Set -t network eth_id gateway <value>	设置编号为 eth_id 的网卡的网关地址
Set -t network eth_id type <value>	设置编号为 eth_id 的网卡的网络类型
Set -h password	显示 Set 命令中 BMC 密码设置部分的帮助信息
Set -t password	修改和设置 BMC 已授权的管理密码
Set -h sol	显示 Set 命令中 SOL 设置部分的帮助信息
Set -t sol eth_id config	设置编号为 eth_id 的网卡的 SOL 是否启用
Set -t sol eth_id baud	设置编号为 eth_id 的网卡的 SOL 通信波特率

以下针对 Get、Set 命令，以及帮助命令进行详细说明。



提示：BMC 配置命令和参数都不区分大小写。

16.1 Get 命令说明

Get 命令可以获得 BMC 当前的三部分设置信息：网络配置信息、用户设置信息、SOL 的配置信息。

Get 命令通用格式：Get -T network/user/sol [<option 1>][<option 2>]

16.1.1 获取当前网络配置

网络配置命令的通用格式：Get -T network <eth_id> [<option>]

Eth_id = 1| 2

Eth_id表示当前服务器上两块网卡标号。1表示获得网卡1，2表示获得网卡2。

Option = ip | subnet | gateway | type

Option 表示获得网络配置的具体内容。ip 表示网卡的 IP 地址，subnet 表示网卡的子网掩码，gateway 表示网卡的网关，type 表示网卡的网络类型。

注意：BMC 配置工具配置的网络信息都是带外管理的网络信息，与操作系统下的网络信息配置没有关系！

命令实例

Get -T network 1

获得 BMC 设置中网卡 1 上所有的网络配置，包括了网络类型、IP 地址、子网

掩码和网关地址等。

Get -T network 1 gateway

获得 BMC 设置中网卡 1 上的网关地址。

Get -T network 2 ip

获得 BMC 设置中网卡 2 上的 IP 地址。

16.1.2 获取当前 SOL 配置

用户设置命令的通用格式：Get -T sol <eth_id> [<option>]

Eth_id = 1| 2

Eth_id表示当前服务器上两块网卡标号。1表示获得网卡1，2表示获得网卡2。

Option = config | baud

config 表示 BMC 的 SOL 功能是否开启；baut 表示当前 BMC 设置的 SOL 通信的波特率是多少。

命令实例

Get -T sol 1 config

获得网卡 1 是否开启 SOL。

Get -T sol 2

获得网卡 2 当前 BMC 设置 SOL 的所有配置信息，包括了 BMC 是否支持 SOL 功能、当前 SOL 通信波特率。

16.2 Set 命令说明

Set 命令可以设置 BMC 当前的三部分设置信息：网络配置信息、用户设置信息、SOL 的配置信息。

Set命令通用格式：Set -T network/user/sol [<option 1>] [<option 2>] <value>

16.2.1 配置网络

网络配置命令的通用格式：Set -T network <eth_id> <option> <value>

Eth_id = 1| 2

Eth_id表示当前服务器上两块网卡标号。1表示设置网卡1，2表示设置网卡2。

Option = ip | subnet | gateway | type

Option 表示获得网络配置的具体内容。ip 表示网卡的 IP 地址，subnet 表示网

卡的子网掩码，gateway 表示网卡的网关，type 表示网卡的网络类型。

Value 表示要设置的数值

[Option] 为 ip 或者 subnet 或者 gateway 时，[value] 的输入要求都为网络 IP 地址格式。

[Option] 为 type 时，[value] 有“Static”、“DHCP”两种。

Static 表示静态 IP 地址类型

DHCP 表示 BMC 通过 DHCP 动态获得 IP 地址

注意：BMC 配置工具配置的网络信息都是带外管理的网络信息，与操作系统下的网络信息配置没有关系！

命令实例

Set -T network 1 ip 192.168.0.10

设置 BMC 网卡 1 的 IP 地址为 192.168.0.10

Set -T network 1 gateway 192.168. 0.1

设置 BMC 网卡 1 的网关地址为 192.168.0.1。

Set -T network 1 subnet 255.255.255.0

设置 BMC 网卡 1 的子网掩码地址为 255.255.255.0。

Set -T network 2 type DHCP

设置 BMC 网卡 2 的网络类型为 DHCP。

提示：默认情况下，服务器网卡 1 的 IP 地址是 192.168.0.2，子网掩码是 255.255.255.0，网关是 0.0.0.0；网卡 2 的 IP 地址是 192.168.0.3，子网掩码是 255.255.255.0，网关是 0.0.0.0。

16.2.2 设置 BMC 管理密码

设置 BMC 管理密码命令的通用格式：Set -T password <value>

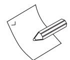
value 表示要设置的密码。

密码是一组 ASCII 字符串，且长度不能超过 16 个字节，区分大小写。

命令实例

Set -T password lenovo

设置当前 BMC 的已授权访问的用户密码为“lenovo”。

**提示：默认情况下，服务器出厂后预设的密码是 lenovo。**

16.2.3 配置 SOL

用户设置命令的通用格式：Set -T sol <eth_id> <option> <value>

Eth_id = 1| 2

Eth_id表示当前服务器上两块网卡标号。1表示设置网卡1，2表示设置网卡2。

Option = config | baud

config 表示 SOL 功能是否启用；baud 表示 SOL 通信的波特率。

Value 表示要设置的值。

[Option] 为 config 时，[value] 输入值是“Enable”或者“Disable”。

[Option] 为 baud 时，[value] 输入值是 1-4 之间的数字。其中，

1 表示 波特率为 19.2 kbps

2 表示 波特率为 38.4 kbps

3 表示 波特率为 57.6 kbps

4 表示 波特率为 115.2 kbps

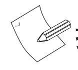
命令实例

Set -T sol 1 config Enable

设置网卡 1 的 BMC 的 SOL，开启 SOL。

Set -T sol 2 baud 2

设置网卡 2 的 BMC 的 SOL 通信的波特率为 38.4 kbps。

**提示：默认情况下，所有网卡的 SOL 功能都启用，并且通信波特率都是 19.2kbps。**

16.3 帮助命令说明

配置工具的内部命令有两种帮助方式。第一种是运行help获得某一条内部命令的帮助信息，第二种方式是其他内部命令中包含了帮助信息。

16.3.1 Help 命令

Help命令的通用格式：help [-C <command name>]

运行help，后面跟上希望知道运行格式的内部命令名称即可。举例说明，用户

键入

help -C set

按 [Enter] 后，屏幕上将显示“set”内部命令的格式和其他帮助信息。

16.3.2 内部命令的帮助

Get 和 Set 内部命令，都有自己的帮助信息。获得内部命令的帮助信息的通用格式：

<command name> -h [<target>]

用户只需键入内部命令名称和<Target>,按下 [Enter]，同样可以获得对该内部命令的帮助信息。

举例说明，用户键入 [Get -T network]，按 [Enter] 后，屏幕上将显示“获得网络设置信息”的命令格式和帮助信息。

第十七章 常见问题解答（FAQ）

17.1 安装与卸载

1. 在win 2003 x64 sp1英文版上安装代理和中心，安装路径选择有中文的目录，会自动去掉文件夹中的中文，如果是纯中文的文件夹，则会安装在它的上一个文件夹下。

请在此机器上的控制面板的语言选项中通过设定非unicode的语言为中文。则可以显示非unicode编码的中文。

2. 管理中心和代理安装包不能在win2003 x64 sp1操作系统上安装，提示NSIS Error ：Error launching installer 。

如果用户通过共享网络安装会因为win2003的安全性原因中断安装过程，从而出现上述错误。请用户下载安装文件到本机安装即可避免此问题。

17.2 运行与配置

3. 管理中心和代理的事件接收端口配一致，但代理通信端口配置的不一致，还是可以收到事件。

只要事件端口配的一致了，就可以接收，而不管管理端口是否一致。他们之间是独立的。

4. 配置完成，运行代理和管理中心，就是无法搜索到服务器，或者对已有的服务器无法监控。

首先，请确认管理中心和管理代理配置是否正确，端口是否一致，通信密钥是否一致。其次，确认管理中心和管理代理所在主机是否正在运行主机防火墙。如果正在运行，则按照手册中的说明进行防火墙配置。

5. 从‘开始-程序’里点击‘监控管理代理’，不能打开代理配置窗口 。

点击后会启动一个托盘程序，用户双击托盘图标，会打开配置窗口。

17.3 服务器搜索

6. 对于linux服务器，分别进行带内和带外搜索，会重复发现，而不会自动识别

为同一台服务器。

在linux操作系统下没有安装BMC驱动，导致无法通过比对带内搜索结果和带外搜索结果比对两次发现的服务器是否是同一台服务器，从而识别为两台不同的服务器。此时，用户仍然可以正常操作。如果用户知道两次发现的结果对应是同一台服务器，可以手工地为服务器添加带外或者带内IP，而不必进行搜索。

可以手工地为服务器添加带外或者带内IP，而不必进行搜索。

7. 搜索服务器的速度有的时候很慢，不仅导致等待时间很长，而且其他人也无法进行搜索。

服务器搜索功能同一时刻只能供一个用户使用。因此，推荐用户在选择搜索范围的时候，尽量事先了解网络中有效IP地址的分布，如果用户选择的搜索范围太大，而这个范围内有效的IP又很少，搜索时间可能会较长，从而导致其他用户无法及时的进行搜索。

17.4 服务器监控

8. 在进行服务器监控的时候，查看进程信息，有时候发现所有进程的CPU利用率总和大于100%。

这是正常的。因为管理代理在获取每个进程CPU利用率的时候，不是同时获取的，存在获取时间上的先后，因此可能造成所有进程总的CPU利用率大于100%。这是Windows操作系统的机制所决定的。造成的误差不影响用户对服务器的管理和诊断。

9. 服务器在开机和关机的时候，页面有时候显示服务器无法管理。这是什么原因？

服务器在开机和关机的时候，会出现带外管理暂时中断的情况，这是因为在开机和关机的时候BMC绑定的网卡会断电并重新加电，此过程会导致管理通信中断。

10. 我的服务器从windows切换到Linux操作系统，管理中心首页“操作系统”的图标没有转换到Linux标志。基本信息也是原来windows的。但是查看服务器的操作系统信息的时候，确显示Linux的信息。这是怎么回事？

如果用户发现这种情况，即说明服务器的操作系统发生了变化，提醒用户更新

系统信息，或者采取其它行动。用户可以通过服务器列表的明细按钮，更新服务器信息，使得服务器操作系统信息得到更新。如果用户不采取任何操作，系统会自动在晚上进行信息更新，确保操作系统信息同步。

11. 有的时候，对于 LINUX 操作系统，无法监视硬件健康信息

由于linux操作系统下没有服务器的BMC驱动，使得无法通过带内方式获得硬件健康信息。因此，如果当前 linux 服务器，有带外管理 ip，那么在带内监控的时候，可以通过带外方式获得健康信息，如果没有带外管理 Ip，那么无法监视健康信息。

12. 对于一个具有带内管理 IP 的服务器，我可以手工添加它的带外管理 IP，实现带外管理吗？

可以。但是，用户在添加带外管理IP的时候，必须确保对应的服务器是正确的。否则，一旦服务器进入带外管理，将会出现混乱。对一台具有带外管理IP的服务器手工添加带内管理 IP 时也要注意同样问题。

17.5 事件与告警

13. 添加错误的服务器带内和带外管理的账号密码，无法管理服务器，但是仍然可以接收事件。

只要这个服务器在管理列表中，就能够收到来自它的事件，不论是否有服务器管理帐号。

14. 两个人用不同的用户账号同时确认同一条事件，均确认成功。那么确认人到底以谁为准？

在两个以上用户同时确认事件的时候，以后一个人的操作为准。

15. 导出事件，查看文件，发现有一部分事件没有发生时间。

BMC芯片记录的事件有一部分是没有发生时间的，只有事件发生的相对时间，即相对于上次服务器启动后的时间。在事件记录中，会注明相对时间，并在事件描述中说明。

16. 我的服务器发生了很多事件，通过浏览器查看事件都能够看到，但是无法接收到短信或者收到邮件。

请确认您是否正确配置了系统邮箱和短信 modem 设备。参见系统配置管理的

13.6 *系统邮箱参数配置*和13.7*GSM Modem 参数配置*。此外，如果要使用短信功能，还必须在管理中心安装好短信 modem，此为选配部件。

17.6 用户与权限

17. 用户连续使用错误的用户名或者口令尝试登录管理中心超过一定的次数,系统就锁定了。

用户连续使用错误的用户名或者口令尝试登录管理中心超过8次，系统会自动锁定 3 分钟。在这 3 分钟内将阻止来自该 IP 的任何登录请求。

18. 在日志过滤的时候，选择其他人，却发现了 admin 帐号的记录 。

这样可以方便的查看是否有人恶意输入admin帐号尝试登陆系统。系统仅仅将失败的登陆归入其他人一类。同理，如果某个用户名开始的时候没有，后来有了，那么在有之前如果使用过的话，都会归入其他人一类。这样，可以有效区分正常登陆和异常登陆。

19. 如何修改 admin 账号的密码？

与其他用户账号密码的修改方式不同，admin账号需要在登录后通过点击界面下面状态区的admin用户名称链接，在弹出的用户信息对话框中修改admin的密码。对于除 admin 以外的账号的密码，可以在用户管理界面中修改。

17.7 系统配置

20. 在系统配置的系统密码策略中，如果一开始设定密码长度大于4位，后来改为长度大于6位。用户使用原来的4位密码仍然可以登录。

如果增强了密码的强度要求，不会对原有的密码强度进行复核和提示。

17.8 和浏览器相关的问题

21. 有的时候在单服务器基本信息页面点 IE 的后退键无法后退。

在用户登陆后第一次进入单服务器管理界面后使用后退功能不能返回,其他时候都可以。

22. 输入了管理中心的地址，但是页面显示的是空白，也没有报错，这是怎么回事？

这是因为浏览器的设置导致的，主要是由于浏览器安全级别设置为高，禁用了

javascript 教本的运行。需要用户修改当前网址的安全区域为本地 Intranet。

23. 输入正确地账号口令登录管理中心后，显示的主页面不正常。

这是因为浏览器的设置导致的，主要是由于浏览器安全级别设置为高，禁用了javascript 教本的运行。需要用户修改当前网址的安全区域为本地 Intranet。

24. 在进行服务器搜索的时候，发现搜索进度条和搜索图标没有展现出动画效果。

这是因为浏览器的设置导致的。需要用户修改Internet选项中的项目，启用“播放网页中的动画”。

25. 系统的弹出式对话框中标题栏的字符显示不全，在最后出现“...”。而有的时候，又能够正确显示，这是什么原因？

这是因为浏览器的设置导致的。需要用户修改当前网址的安全区域为本地Intranet。

26. 用户在登录管理中心使用过程中，管理中心重启，在页面访问的时候会出现要求重新登录的页面。

如果服务器重新启动，就会发生这种情况。

17.9 服务器远程控制

27. IDER 能够支持哪些操作系统？

目前，用户的被管理服务器可以在windows下使用IDER功能，尚不能在linux和 DOS 下使用 IDER 功能。

28. SOL 能够支持哪些操作系统？

目前，用户的被管理服务器可以在开机POST过程中，RAID/BIOS设置时，以及DOS环境下使用SOL功能，尚不能在linux和windows下使用SOL功能。

附录 A 术语

BMC	Baseboard Management Controller，主板管理控制器，是集成在主板上的一颗服务器管理芯片，用于采集和监视服务器的硬件健康信息，以及允许管理员通过主板上的网卡直接对服务器进行远程控制。
DMZ	Demilitarized Zone，隔离区，非军事化区。是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部Intranet网络和外部Internet网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。在现代企业网络中，DMZ 设置是十分常见的。
IDER	IDE Redirection，IDE 设备重定向。利用服务器主板上的BMC芯片，将位于网络中的远程的IDE设备虚拟为服务器本地的IDE设备。这些IDE 设备包括软驱、光驱、硬盘，等等。
SOL	Serial over LAN，基于网络的串口重定向。利用服务器主板上的BMC芯片，将服务器的串口信息重定向到位于网络的远程终端上，实现POST 过程、BIOS 设置、DOS 操作界面的远程重定向。
带内管理	In-band Management，指基于操作系统的服务器管理。
带外管理	Out-of-band Management，指不基于操作系统，直接利用BMC实现的服务器管理。